IDEMIA

ID-One PIV 243 & FIDO 213

FIPS 140-3 Non-Proprietary Security Policy



Document Version 1.3
Last update: 2026-11-16

Prepared by:

atsec information security corporation
4516 Seton Center Parkway, Suite 250
Austin, TX 78759
www.atsec.com

© 2026 IDEMIA / atsec information security.

This document can be reproduced and distributed only whole and intact, including this copyright notice.

Table of Contents

1 General 5
1.1 Overview 5
1.2 Security Levels 5
2 Cryptographic Module Specification 6
2.1 Description 6
2.2 Tested and Vendor Affirmed Module Version and Identification 8
2.3 Excluded Components 8
2.4 Modes of Operation 8
2.5 Algorithms 9
2.6 Security Function Implementations 12
2.7 Algorithm Specific Information 15
2.8 RBG and Entropy 16
2.9 Key Generation 17
2.10 Key Establishment 17
2.11 Industry Protocols 17
3 Cryptographic Module Interfaces 18
3.1 Ports and Interfaces 18
3.2 Trusted Channel Specification 18
3.3 Control Interface Not Inhibited 18
4 Roles, Services, and Authentication 19
4.1 Authentication Methods 19
4.2 Roles 21
4.3 Approved Services 22
4.4 Non-Approved Services 80
4.5 External Software/Firmware Loaded 80
5 Software/Firmware Security 81
5.1 Integrity Techniques 81
5.2 Initiate on Demand 81
6 Operational Environment 82
6.1 Operational Environment Type and Requirements 82
7 Physical Security 83
7.1 Mechanisms and Actions Required 83
7.2 EFP/EFT Information 83

© 2026 IDEMIA / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

7.3 Hardness Testing Temperature Ranges 83
8 Non-Invasive Security 84
9 Sensitive Security Parameters Management 85
9.1 Storage Areas 85
9.2 SSP Input-Output Methods 85
9.3 SSP Zeroization Methods 86
9.4 SSPs 87
9.5 Transitions 110
10 Self-Tests 111
10.1 Pre-Operational Self-Tests 111
10.2 Conditional Self-Tests 111
10.3 Periodic Self-Test Information 113
10.4 Error States 115
11 Life-Cycle Assurance 117
11.1 Installation, Initialization, and Startup Procedures 117
11.1.1 Initialization 117
11.1.2 Startup Procedures 117
11.2 Administrator Guidance 117
11.3 Non-Administrator Guidance 117
11.4 Design and Rules 117
11.5 End of Life 117
12 Mitigation of Other Attacks 118
12.1 Attack List 118
12.2 Guidance and Constraints 118
References 119

© 2026 IDEMIA / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

List of Tables

Table 1: Security Levels 5
Table 2: Tested Module Identification – Hardware 8
Table 3: Modes List and Description 9
Table 4: Approved Algorithms 11
Table 5: Vendor-Affirmed Algorithms 11
Table 6: Non-Approved, Allowed Algorithms with No Security Claimed 12
Table 7: Security Function Implementations 15
Table 8: Entropy Certificates 16
Table 9: Entropy Sources 16
Table 10: Ports and Interfaces 18
Table 11: Authentication Methods 19
Table 12: Roles 21
Table 13: Approved Services 79
Table 14: Mechanisms and Actions Required 83
Table 15: EFP/EFT Information 83
Table 16: Hardness Testing Temperatures 83
Table 17: Storage Areas 85
Table 18: SSP Input-Output Methods 85
Table 19: SSP Zeroization Methods 86
Table 20: SSP Table 1 96
Table 21: SSP Table 2 110
Table 22: Pre-Operational Self-Tests 111
Table 23: Conditional Self-Tests 113
Table 24: Pre-Operational Periodic Information 113
Table 25: Conditional Periodic Information 115
Table 26: Error States 116

List of Figures

Figure 1: Depiction of Physical Form 6
Figure 2: Block Diagram 7
Figure 3: Bottom View 8
Figure 4: Top View 8

© 2026 IDEMIA / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

1 General

1.1 Overview

This document defines the Security Policy for the ID-One PIV 243 & FIDO 213 cryptographic module from IDEMIA when configured by IDEMIA in FIPS 140-3 Level 2 mode of operation, and hereafter denoted the module. The module, validated to FIPS 140-3 overall Security Level 2, is a single chip module implementing the Global Platform operational environment, with Card Manager and both ID-One PIV 243 and FIDO 213 Applets.

1.2 Security Levels

The FIPS 140-3 security levels for the module are as follows:

Section	Title	Security Level
1	General	2
2	Cryptographic module specification	2
3	Cryptographic module interfaces	2
4	Roles, services, and authentication	3
5	Software/Firmware security	2
6	Operational environment	N/A
7	Physical security	3
8	Non-invasive security	N/A
9	Sensitive security parameter management	2
10	Self-tests	3
11	Life-cycle assurance	3
12	Mitigation of other attacks	3
	Overall Level	2

Table 1: Security Levels

© 2026 IDEMIA / atsec information security.

This document can be reproduced and distributed only whole and intact, including this copyright notice.

2 Cryptographic Module Specification

2.1 Description

Purpose and Use:

The ID-One PIV & FIDO module implements cryptographic services for the Global Platform operational environment, with Card Manager and two applets, ID-One PIV 243 and FIDO 213 from IDEMIA.
Module Type: Hardware
Module Embodiment: Single Chip

Cryptographic Boundary:

The module is designed to be embedded into a plastic card body, with a contact plate and/or contactless antenna connections, or in a USB token or other standard IC packaging, such as SOIC, QFN or MicroSD.

The physical form of the module is depicted in Figure 1 below. The cryptographic boundary of the module is the surface and edges of the die and associated bond pads for the module's interfaces, shown as circles in the figure. See Table 12: Ports and Interfaces for the function of each interface.

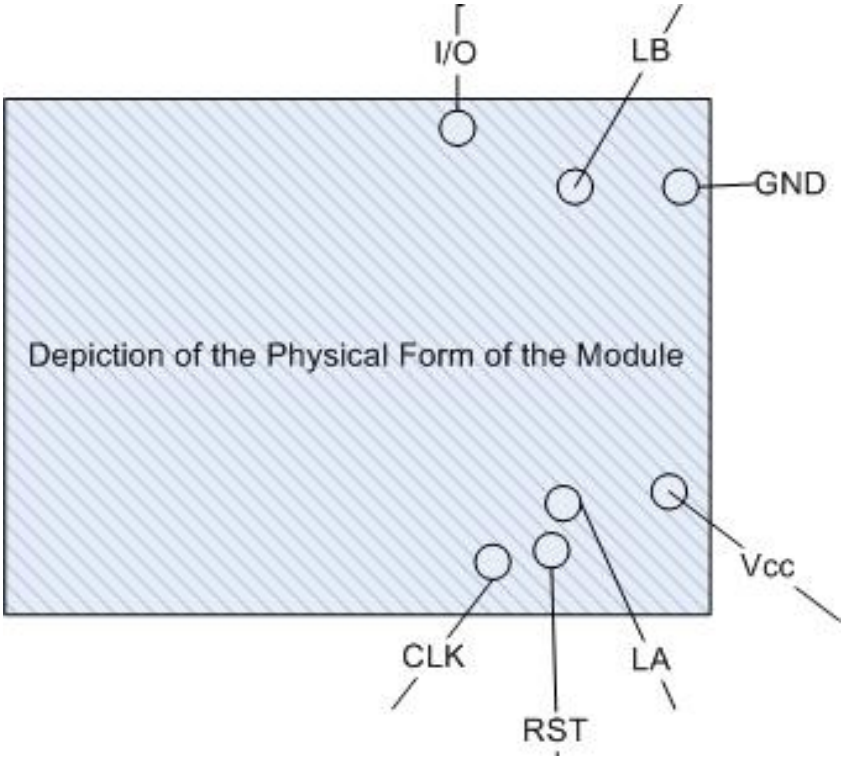


Figure 1: Depiction of Physical Form

© 2026 IDEMIA / atsec information security.

This document can be reproduced and distributed only whole and intact, including this copyright notice.

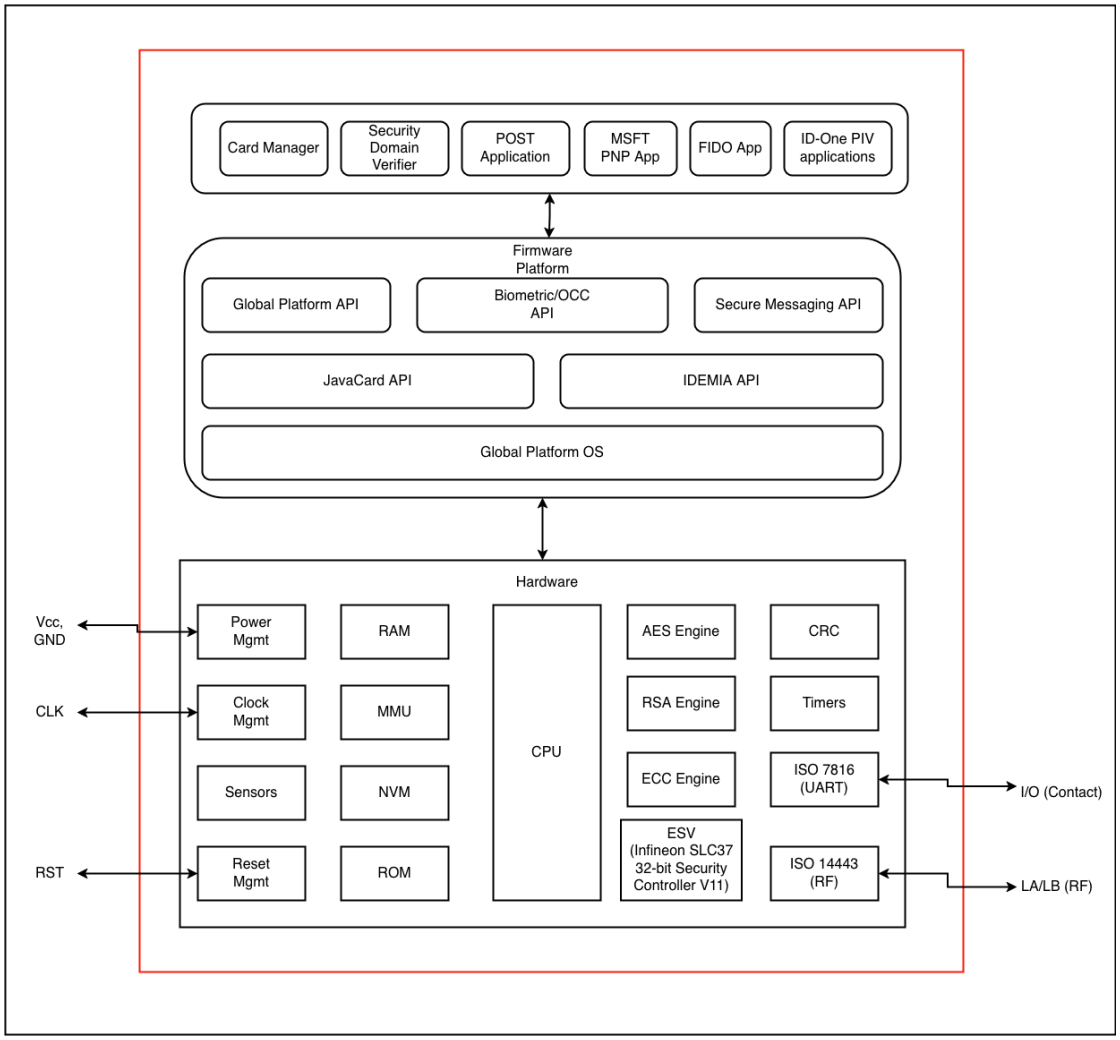


Figure 2: Block Diagram

Section 4 describes applet functionality in greater detail. The JavaCard and Global Platform APIs are internal interfaces available only to applets. Only applet services are available at the card edge (the interfaces that cross the cryptographic boundary). In the figure above, the Security Domain Verifier prevents loading an unauthorized (unsigned) code package into the module and does not provide separate services.

The POST application provides on-demand execution of the conditional Cryptographic Algorithms Self-Test (CAST) and the MSFT PNP application provides identification of the associated mini-driver when the module is used within a Microsoft Windows Environment. All code is executed from ROM and NVM.

The module provides hardware engines AES, RSA, ECC, a hardware entropy source validated to SP800-90B, and a non-cryptographic CRC engine. The communications options for contact and contactless configurations are present in the physical circuitry of all members of the processor family but are selectively enabled during module manufacturing.

© 2026 IDEMIA / atsec information security.

This document can be reproduced and distributed only whole and intact, including this copyright notice.

2.2 Tested and Vendor Affirmed Module Version and Identification

Tested Module Identification – Hardware:

Model and/or Part Number	Hardware Version	Firmware Version	Processors	Features
Cosmo X FIPS	09A4D1	418424 (for PIV 243 applet) and 203812 (for FIDO 213 applet)	32-bit Arm®	Contact-Only, Contactless-Only or Dual Interface

Table 2: Tested Module Identification – Hardware

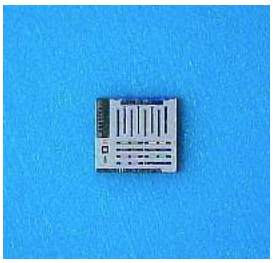


Figure 3: Bottom View

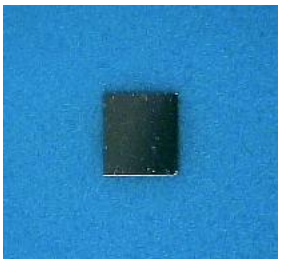


Figure 4: Top View

2.3 Excluded Components

There are no components within the cryptographic boundary excluded from the FIPS 140-3 requirements.

2.4 Modes of Operation

Modes List and Description:

Mode Name	Description	Type	Status Indicator
NPIVP & FIDO (612431XX01)	The NPIVP (NIST Personal Identity Verification Program) & FIDO configuration is FIPS 201-3 compliant and designed to be used by US Federal Agencies for PIV, PIV-I Cards and FIDO Cards and Keys.	Approved	The indicator of mode of operations of a given ID-One PIV instance can be retrieved at any time using the READ BINARY command (PIV Info Unauthenticated service) on its Elementary file (EF) with SFI=01. The module will return "Running in FIPS140-3 Level 2 Mode of Operations" in ASCII
CIV FIPS & FIDO (612432XX01)	The CIV FIPS & FIDO is the configuration for Commercial uses. It is backward compatible with NPIVP but offers enhanced functionality and access conditions	Approved	The indicator of mode of operations of a given ID-One PIV instance can be retrieved at any time using the READ BINARY command (PIV Info Unauthenticated service) on its Elementary file (EF) with SFI=01. The

© 2026 IDEMIA / atsec information security.

This document can be reproduced and distributed only whole and intact, including this copyright notice.

Mode Name	Description	Type	Status Indicator
	for additional use cases. It also offers FIDO functionalities.		module will return "Running in FIPS140-3 Level 2 Mode of Operations" in ASCII
CIV+ & FIDO (612432XX11)	The CIV+ & FIDO configuration is the CIV configuration with an additional instance of the ID-One PIV® applet, called "eStickers", for additional data and keys outside of HSPD#12 interoperability requirements specified by FIPS 201. It also offers FIDO functionalities.	Approved	The indicator of mode of operations of a given ID-One PIV instance can be retrieved at any time using the READ BINARY command (PIV Info Unauthenticated service) on its Elementary file (EF) with SFI=01. The module will return "Running in FIPS140-3 Level 2 Mode of Operations" in ASCII

Table 3: Modes List and Description

The mode of operation is defined by IDEMIA during manufacturing and cannot be changed. The module does not allow the changing of modes after manufacturing.

2.5 Algorithms

Approved Algorithms:

The module only implements approved algorithms and does not implement any non-approved algorithms. Therefore, the module only has approved mode of operation.

Algorithm	CAVP Cert	Properties	Reference
AES-CBC	A4945	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CMAC	A4945	-	SP 800-38B
AES-ECB	A4945	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
Counter DRBG	A4945	Prediction Resistance - No Mode - AES-256 Derivation Function Enabled - Yes	SP 800-90A Rev. 1
ECDSA KeyGen (FIPS186-4)	A4945	Curve - P-224, P-256, P-384, P-521 Secret Generation Mode - Testing Candidates	FIPS 186-4
ECDSA KeyVer (FIPS186-4)	A4945	Curve - P-224, P-256, P-384, P-521	FIPS 186-4
ECDSA SigGen (FIPS186-4)	A4945	Component - No, Yes Curve - P-224, P-256, P-384, P-521	FIPS 186-4

© 2026 IDEMIA / atsec information security.

This document can be reproduced and distributed only whole and intact, including this copyright notice.

Algorithm	CAVP Cert	Properties	Reference
		Hash Algorithm - SHA2-224, SHA2-256, SHA2-384, SHA2-512	
ECDSA SigVer (FIPS186-4)	A4945	Component - No, Yes Curve - P-224, P-256, P-384, P-521 Hash Algorithm - SHA2-224, SHA2-256, SHA2-384, SHA2-512	FIPS 186-4
HMAC-SHA-1	A4945	Key Length - Key Length: 8-1016 Increment 8	FIPS 198-1
HMAC-SHA2-256	A4945	Key Length - Key Length: 8-1016 Increment 8	FIPS 198-1
HMAC-SHA2-512	A4945	Key Length - Key Length: 8-1016 Increment 8	FIPS 198-1
KAS-ECC CDH-Component (CVL)	A4945	-	SP 800-56A Rev. 3
KAS-ECC Sp800-56Ar3	A4945	Domain Parameter Generation Methods - P-256, P-384, P-521 Function - Key Pair Generation Scheme - onePassDh - KAS Role - Responder KDF Methods - oneStepKdf - Key Length - 1024	SP 800-56A Rev. 3
KAS-ECC Sp800-56Ar3	A8128	Domain Parameter Generation Methods - P-256 Function - Full Validation Scheme - ephemeralUnified - KAS Role - Responder KDF Methods - twoStepKdf - Key Length - 256	SP 800-56A Rev. 3
KDF SP800-108	A4945	KDF Mode - Counter Supported Lengths - Supported Lengths: 64, 256	SP 800-108 Rev. 1
RSA Decryption Primitive Sp800-56Br2 (CVL)	A4945	Modulo - 2048, 3072, 4096	SP 800-56B Rev. 2

© 2026 IDEMIA / atsec information security.

This document can be reproduced and distributed only whole and intact, including this copyright notice.

Algorithm	CAVP Cert	Properties	Reference
RSA KeyGen (FIPS186-4)	A4945	Key Generation Mode - B.3.6 Modulo - 2048, 3072, 4096 Primality Tests - Table C.3 Private Key Format - Chinese Remainder Theorem	FIPS 186-4
RSA SigGen (FIPS186-4)	A4945	Signature Type - PKCSPSS Modulo - 2048, 3072, 4096	FIPS 186-4
RSA Signature Primitive (CVL)	A4945	Private Key Format - crt	FIPS 186-4
RSA SigVer (FIPS186-4)	A4945	Signature Type - PKCSPSS Modulo - 1024, 2048, 3072, 4096	FIPS 186-4
SHA2-224	A4945	Message Length - Message Length: 0-65536 Increment 8 Large Message Sizes - 1	FIPS 180-4
SHA2-256	A4945	Message Length - Message Length: 0-65536 Increment 8 Large Message Sizes - 1	FIPS 180-4
SHA2-384	A4945	Message Length - Message Length: 0-65536 Increment 8 Large Message Sizes - 1	FIPS 180-4
SHA2-512	A4945	Message Length - Message Length: 0-65536 Increment 8 Large Message Sizes - 1	FIPS 180-4

Table 4: Approved Algorithms

Vendor-Affirmed Algorithms:

Name	Properties	Implementation	Reference
CKG	Key Type:Symmetric and Asymmetric	N/A	Key Generation Compliant with SP 800-133Rev2 section 4 example 1

Table 5: Vendor-Affirmed Algorithms

Non-Approved, Allowed Algorithms:

N/A for this module.

© 2026 IDEMIA / atsec information security.

This document can be reproduced and distributed only whole and intact, including this copyright notice.

Non-Approved, Allowed Algorithms with No Security Claimed:

Name	Caveat	Use and Function
RSA Deobfuscation	RSA Deobfuscation Operation with 1024-bit modulus allowed per IG 2.4.A	RSA Deobfuscation

Table 6: Non-Approved, Allowed Algorithms with No Security Claimed

Non-Approved, Not Allowed Algorithms:

N/A for this module.

2.6 Security Function Implementations

Name	Type	Description	Properties	Algorithms
AES-ECB	BC-UnAuth	Symmetric encryption and Decryption	Key Size:128, 192, 256 bits Key Strength:128, 192, 256 bits	AES-ECB: (A4945)
AES-CBC	BC-UnAuth	Symmetric encryption and Decryption	Key Size:128, 192, 256 bits Key Strength:128, 192, 256 bits	AES-CBC: (A4945)
AES-CMAC	MAC	Message Authentication Code	Key Size:128, 192, 256 bits Key Strength:128, 192, 256 bits	AES-CMAC: (A4945)
CTR DRBG	DRBG	CTR_DRBG using AES-256	Derivation Function:Enabled Prediction Resistance:No Key Size:256 bits Key Strength:256 bits	Counter DRBG: (A4945)
ECDSA keyGen	AsymKeyPair-KeyGen CKG	ECDSA key generation using Testing Candidates	Curves:P-224, P-256, P-384, P-521 Strength:112, 128, 192, 256 bits	ECDSA KeyGen (FIPS186-4): (A4945) CKG: ()
ECDSA keyVer	AsymKeyPair-KeyVer	ECDSA key verification	Curves:P-224, P-256, P-384, P-521 Strength:112, 128, 192, 256 bits	ECDSA KeyVer (FIPS186-4): (A4945)

© 2026 IDEMIA / atsec information security.

This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Type	Description	Properties	Algorithms
ECDSA sigGen	DigSig-SigGen	ECDSA Digital Signature Generation	Message Digest:SHA2-224, SHA2-256, SHA2-384, SHA2-512 Curves:P-224, P-256, P-384, P-521 Strength:112, 128, 192, 256 bits	ECDSA SigGen (FIPS186-4): (A4945)
ECDSA sigGen component	DigSig-SigGen	ECDSA Digital Signature Generation Component	Curves:P-224, P-256, P-384, P-521 Strength:112, 128, 192, 256 bits	ECDSA SigGen (FIPS186-4): (A4945)
ECDSA sigVer	DigSig-SigVer	ECDSA Digital Signature Verification	Message Digest:SHA2-224 Curves:P-224, P-256, P-384, P-521 Strength:112, 128, 192, 256 bits	ECDSA SigVer (FIPS186-4): (A4945)
KAS-ECC	KAS-Full	ECDH Key Agreement Scheme	Scheme:onePassDh KDF Method:oneStepKdf Curves:P-256, P-384, P-521 Strength:128, 192, 256 bits	KAS-ECC Sp800-56Ar3: (A4945)
KAS-ECC CDH Component	KAS-SSC	ECDH Component	Curves:P-224, P-256, P-384, P-521 Strength:112, 128, 192, 256 bits	KAS-ECC CDH-Component: (A4945)
RSA keyGen	AsymKeyPair-KeyGen CKG	RSA Key Generation	Generation Method:A.1.6 Probable Primes with conditions based on Auxiliary Probable Primes Key Size:2048, 3072, 4096 bits Key Strength:112, 128, 150 bits	RSA KeyGen (FIPS186-4): (A4945) CKG: ()
RSA sigGen	DigSig-SigGen	RSA Digital Signature Generation	Scheme:PSS Key Size:2048, 3072, 4096 bits	RSA SigGen (FIPS186-4): (A4945)

© 2026 IDEMIA / atsec information security.

This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Type	Description	Properties	Algorithms
			Key Strength:Strength: 112, 128, 150 bits	
RSA sigPrim	DigSig-SigGen	RSA Digital Signature Generation primitive	Key Size:2048, 3072, 4096 bits Key Strength:112, 128, 150 bits	RSA Signature Primitive: (A4945)
RSA sigVer	DigSig-SigVer	RSA Digital Signature Verification	Scheme:PSS using SHA2-256 Key Size:2048 bits Key Strength:112 bits	RSA SigVer (FIPS186-4): (A4945)
RSA Decryption Primitive (CVL)	KTS-Wrap	RSA Decryption Primitive (CVL)	Key Size:2048, 3072, 4096 bits Key Strength:112, 128, 150 bits	RSA Decryption Primitive Sp800-56Br2: (A4945)
HMAC	MAC	Message Authentication Code using HMAC with SHA	Key Size:112 to 1016 bits Key Strength:112 to 1016 bits	HMAC-SHA-1: (A4945) HMAC-SHA2-256: (A4945) HMAC-SHA2-512: (A4945)
KBKDF SP 800-108	KBKDF	Key Based Key Derivation with Counter	Fixed Data Order:Middle Fixed Data Key Size:128, 192, 256 bits Key Strength:128, 192, 256 bits	KDF SP800-108: (A4945)
SHA	SHA	Message Digest Generation using SHA2-224, SHA2-256, SHA2-384, SHA2-512		SHA2-224: (A4945) SHA2-256: (A4945) SHA2-384: (A4945) SHA2-512: (A4945)
KTS (AES + CMAC) key wrapping/unwrapping	KTS-Unwrap KTS-Wrap	Symmetric key wrapping/unwrapping	Key Size:128, 192, 256 bits Key Strength:128, 192, 256 bits	AES-CBC: (A4945) AES-CMAC: (A4945)

© 2026 IDEMIA / atsec information security.

This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Type	Description	Properties	Algorithms
KTS (AES + HMAC) key wrapping/unwrapping	KTS-Unwrap KTS-Wrap	Symmetric key wrapping/unwrapping for FIDO	Key Size:128, 192, 256 bits Key Strength:128, 192, 256 bits	AES-CBC: (A4945) SHA2-256: (A4945)
KAS-ECC (FIDO)	KAS-Full	ECDH Key Agreement Scheme within PIV/UV Auth Protocol Two	Scheme:onePassDh KDF Method:twoStepKdf Curves:P-256, P-384, P-521 Strength:128, 192, 256 bits	KAS-ECC Sp800-56Ar3: (A8128)

Table 7: Security Function Implementations

2.7 Algorithm Specific Information

IG C.K: The module includes CAVP certificates using FIPS 186-4 tests done prior to the IG C.K transition date of Feb 5th, 2024, and are mathematically identical to FIPS 186-5 CAVP tests, hence the module claims FIPS 186-5 compliance for these tests.

The module does not establish SSPs using an approved key agreement scheme (KAS). However, it does offer some or all of the underlying KAS cryptographic functionality to be used by an external operator/application as part of an approved KAS.

The module provides services for the following CVLs for external use cases.

- KAS-ECC CDH-Component (CVL) - shall only be used within the context of an SP 800-56Arev3 KAS.
- RSA Decryption Primitive (CVL) - shall only be used within the context of a SP 800-56Brev2 KTS

Compliance to SP 800-56ARev3 assurances

For KAS-ECC, the module satisfies IG D.F Scenario 2 path (2) (i.e., tested compliance with One Pass DH key agreement schemes followed by the derivation of the key as shown in Section 5.8 of SP 800-56Arev3). The key derivation function complies to SP 800-56C rev2 (i.e., One-Step KDF). Furthermore, the module obtained the appropriate assurances, as required in Sections 5.6.2 of SP 800-56A rev3.

5.6.2.1 Assurances Required by a Key Pair Owner:

5.6.2.1.1 Owner Assurance of Correct Generation: The module performs key generation for ephemeral keys. Using the key generation algorithm validated by the CAVP (ECDSA KeyGen Cert. #A4945). For static keys, a trusted third party (TTP) generates the key pair and securely enters the module using SP800-38F key wrapping (AES + CMAC). The module will perform a pairwise consistency check upon generating ECDH keys.

5.6.2.1.2 Owner Assurance of Private-Key Validity: For ephemeral key pair, the module provides the assurance since the module generates it. For static key pairs, after receiving the key pair, the module performs a separate check to determine that the private key is in the correct interval.

5.6.2.1.3 Owner Assurance of Public-Key Validity: For both static and ephemeral key pairs, the module performs a full public-key validation as a separate process from the key-pair generation process.

© 2026 IDEMIA / atsec information security.

This document can be reproduced and distributed only whole and intact, including this copyright notice.

5.6.2.1.4 Owner Assurance of Pair-wise Consistency: The module performs a pair-wise consistency test when the module generates ephemeral key pairs and when static key-pairs are entered into the module.

5.6.2.1.5 Owner Assurance of Possession of the Private Key: For ephemeral key pairs, The owner generates the key pair as specified in Section 5.6.1 and for ephemeral key pairs, the module performs a pair-wise consistency test when the key pairs are entered.

5.6.2.2 Assurances Required by a Public Key Recipient

5.6.2.2.1 Recipient's assurance Static Public-Key Validity: The module makes used of approved EC curves listed in SP800-140D and performs a successful full public-key validation of the received public key i.e., ECC Full Public-Key Validation Routine specified in SP800-56A rev3 section 5.6.2.3.3.

5.6.2.2.2 Recipient Assurance of Ephemeral Public-Key Validity: Not applicable. The module generates ephemeral keys and does not ever receive them.

5.6.2.2.3 Recipient's assurance of owner's possession of private key can be met via the use of a Trusted Third party that requires the key confirmation procedure. Both of which are handled by the entity outside of the module that requested the ECDH Key Agreement service from the module. That is, such checks are out of the module's scope.

5.6.2.2.4 Recipient Assurance of the Owner's Possession of an Ephemeral Private Key: Not applicable. The module generates ephemeral keys and does not ever receive them.

5.6.2.3 Public Key Validation Routines

The module performs the required public key validation before initiating the handshake following 5.6.2.3.3 ECC Full Public-Key Validation Routine.

2.8 RBG and Entropy

Cert Number	Vendor Name
E107	Infineon Technologies AG

Table 8: Entropy Certificates

Name	Type	Operational Environment	Sample Size	Entropy per Sample	Conditioning Component
Infineon SLC37 32-bit Security Controller V11 Entropy Source	Physical	SLC37 32-bit Security Controller V11	32-bit blocks which can be concatenated	13.376-bits per 32-bit block	non-vetted conditioning function

Table 9: Entropy Sources

RNG Information: The module implements an approved SP 800-90Ar1 Deterministic Random Bit Generator in the form of CTR_DRBG. The DRBG seed is generated from the SP 800-90B entropy source. All configuration of the entropy source is automatically set by the module at startup.

© 2026 IDEMIA / atsec information security.

This document can be reproduced and distributed only whole and intact, including this copyright notice.

2.9 Key Generation

The module implements key generation services for RSA, ECDSA, EC Diffie-Hellman, and AES keys in compliance to SP800-133rev2 Cryptographic Key Generation (CKG, vendor affirmed).

2.10 Key Establishment

The module provides an approved SP800-56Arev3 EC Diffie-Hellman Key Agreement Scheme that is fully compliant with IG D.F scenario 2 path (2).

The module provides an approved SP800-38F Key Transport that is fully compliant to IG D.G i.e., employing an approved key-wrapping technique using a “combination” method: AES-CBC together with an approved authentication method AES-CMAC.

2.11 Industry Protocols

The GP Secure Channel Protocol '03' establishment provides mutual authentication service as well as establishment of a secure channel to protect confidentiality and integrity of the transmitted data.

The PIV Secure Messaging protocol defined in SP800-73-4 and ANSI 504-1 establishes a secure channel to protect confidentiality and integrity of transmitted information and allows the off-card entity initiating the PIV Secure Messaging to authenticate the module. Unlike GP Secure Channel, the PIV Secure Messaging does not allow the module to authenticate the off-card entity.

The PIV Secure Messaging protocol conforms to SP800-56A for the establishment of a shared secret and key derivation for session keys.

© 2026 IDEMIA / atsec information security.

This document can be reproduced and distributed only whole and intact, including this copyright notice.

3 Cryptographic Module Interfaces

3.1 Ports and Interfaces

Physical Port	Logical Interface(s)	Data That Passes
RST [ISO 7816: Reset] Not available in contactless-only configurations	Control Input	None
CLK [ISO 7816: Clock] Not available in contactless-only configurations	Control Input	None
I/O [ISO 7816: Input/Output] Not available in contactless-only configurations	Data Input Data Output Control Input Status Output	APDU Command data field; ATR and APDU Response data field; APDU Header (CLA INS P1-P2); Status Word SW1-SW2
LA, LB [ISO 1443: Antenna] (Not available in contact-only configurations)	Data Input Data Output Control Input Status Output	APDU Command data field; ATR and APDU Response data field; APDU Header (CLA INS P1-P2); Status Word SW1-SW2
Vcc, GND [ISO 7816: Supply voltage] (Not available in contactless-only configurations)	Power	None

Table 10: Ports and Interfaces

The module does not implement any control output interface.

3.2 Trusted Channel Specification

The module does not implement a trusted channel.

3.3 Control Interface Not Inhibited

The control interface is inhibited while in the error state without any exceptions.

© 2026 IDEMIA / atsec information security.

This document can be reproduced and distributed only whole and intact, including this copyright notice.

4 Roles, Services, and Authentication

4.1 Authentication Methods

Method Name	Description	Security Mechanism	Strength Each Attempt	Strength per Minute
GP Secure Channel Protocol Authentication	Provides authentication for the CO role	AES-CMAC (A4945)	1/(2^128)	9/(2^128)
PIV Symmetric Key Authentication	Provides authentication for the PIV Application Administrator	AES-ECB (A4945)	1/(2^128)	9/(2^128)
PIV Secret Value Authentication	Provides authentication for the user	PIN Input	1/((10^6)(11^2)) or 1/((94^6)(95^6))	15/((10^6)(11^2)) or 15/((94^6)(95^6))
BIO Authentication	Biometric person authentication On-Card-Comparison (OCC)	Biometric authentication using facial, fingerprint, or iris.	See section 4.1	See section 4.1

Table 11: Authentication Methods

GP Secure Channel Protocol Authentication Method

The Secure Channel Protocol authentication method is provided by the Secure Channel service. The SD-DAK and SD-DMK keys are used to derive the SC-ENC and SC-C-MAC keys, respectively. The off-card entity participating in the mutual authentication sent a 64-bit challenge to the Smart Card together with the key set version to use. The Smart Card together with the key set version to use. generates its own challenge and computes a 64-bit cryptogram with SC-C-MAC key and both challenges. The Smart Card cryptogram and challenge are sent to the off-card entity which checks the Smart Card cryptogram and creates its own 64-bit cryptogram with both challenges. A 64-bit message authentication code (MAC) is also computed on the command containing the off-card entity cryptogram with AES-CMAC and SC-C-MAC key, the MAC is concatenated to the command, and the command is sent to the Smart Card. The Smart Card checks the message authentication code and compares the received cryptogram to the calculated cryptogram. If all of this succeeds, the two participants are mutually authenticated (the external entity is authenticated to the Module in the CO role).

The probability that a random attempt will succeed using this authentication method is:

- $1/(2^{128})$ = 2.9E-39 (MAC||cryptogram using a 128-bit block for authentication)

The module enforces a “slowdown mechanism” that increases the response time between two authentications attempts following a failed authentication, such that no more than nine (9) attempts are possible in a one-minute period. The probability that a random attempt will succeed over a one-minute interval is:

- $9/(2^{128})$ = 2.6E-38 (MAC||cryptogram using a 128-bit block for authentication)

© 2026 IDEMIA / atsec information security.

This document can be reproduced and distributed only whole and intact, including this copyright notice.

GP Secure Channel Protocol establishment provides mutual authentication service as well as establishment of a secure channel to protect confidentiality and integrity of the transmitted data.

GP Secure Channel Protocol Authentication Method using Pseudo Random

The module supports Global Platform Authentication using an optional Pseudo Random method, described in "GP Secure Channel Protocol '03' Card Specification v2.2 Amendment D". The CO can determine the challenge which will be generated by the module. The use of a pseudo-random card challenge allows the offline preparation of personalization scripts while the module is not present and the processing of these scripts on the module without an online connection to the entity that prepared the scripts. When this option is called, the card challenge mentioned in the above section is the result of an AES-CMAC computed on a 24-bit counter value, a constant AID value, and a host challenge. The counter is initialized to 0 when the key is created or replaced, and the module returns an error when the counter reached 2^{24}-1.

The use of the optional pseudo random card challenge does not impact the probabilities listed above.

PIV Symmetric Key Authentication Method

The external entity obtains a 16-byte challenge from the module, encrypts the challenge, and sends the cryptogram to the module. The module decrypts the cryptogram, and the external entity is authenticated if the decrypted value matches the challenge. This method is used by the *PIV Application Administrator Authentication* services. The minimum key strength used for this method is AES-128, using 16 bytes (a single AES block).

The probability that a random attempt will succeed using this authentication method is:

- $1/(2^{128}) = 2.9E-39$

The module enforces a “slowdown mechanism” that increases the response time between two authentication attempts following a failed authentication, such that no more than nine (9) attempts are possible in a one-minute period. The probability that a random attempt will succeed over a one-minute interval is:

- $9/(2^{128}) = 2.6E-38$

PIV Secret Value Authentication Method

The external entity submits an identifier and corresponding secret value. The format of the secret value is checked for conformance to a defined format template (Numeric in ASCII, Alphanumeric with at least one upper case, one lower case, one digit and one special character, Alphanumeric with at least three of the previous 4 categories, Numeric in BCD, HEX value, etc.), and for its minimum number of characters before padding. If the check passes, the module compares all eight (8) or sixteen (16) bytes to the appropriate stored reference instance (e.g. Cardholder PIN, Pin Unblocking Key or Administrator PIN). The enforcement of minimum number of characters before padding is not the same as a fixed length for the secret. For example, a minimum of six (6) characters means secrets can be created from six (6) to eight (8) characters, determined by the user (or six (6) to sixteen (16) if the module was configured during production to support 16-byte PINs).

The minimum length of the PIN is 6 bytes and the maximum 8 or 16 bytes depending on configuration.

The worst-case scenario permitted by the module is a minimum length of six (6) characters with the Numeric in ASCII character set and a maximum length of eight (8) characters. The character space for the first six (6) bytes in this scenario is 10 (the values ‘30’ through ‘39’ are permitted) and in the last two (2) characters is 11 (the values ‘30’ through ‘39’ and ‘FF’ are permitted). The probability that a random attempt will succeed using this authentication method is:

- $1/(10^6 * 11^2) = 8.3E-9$

© 2026 IDEMIA / atsec information security.

This document can be reproduced and distributed only whole and intact, including this copyright notice.

The maximum number of consecutive failed authentication attempts can be configured up to 15, so the probability that a random attempt will succeed over a one-minute interval is:

- $15/(10^6 * 11^2) = 1.2E-7$

BIO Authentication method

The module performs a biometric person authentication On-Card-Comparison (OCC) using one of the following methods:

- A live fingerprint template as defined by FIPS 201-2. (BIT Format Owner = 0x0101)
- An iris template. (BIT Format Owner = 0x001D)
- A facial template. (BIT Format Owner = 0x001D)

The default threshold applied to scores from the fingerprint OCC algorithms has been set to achieve false match rates (FMR) at or below the respective values defined by NIST in Table 16 of SP800-76-2, i.e., an FMR of 0.001 for on-card fingerprint minutia matching.

As required by SP800-76-2 section 5.7.4.1, the on-card-matching algorithm matches single-finger native templates with False Non-Match Rate (FNMR) less than or equal to 0.02 when the FMR is at or below 0.0001.

The default threshold for Facial OCC has been set to achieve false match rates (FMR) of 0.001.

The default threshold for Iris OCC has been set to achieve false match rates (FMR) of 0.001.

The above default threshold values can be adjusted by the Crypto-Officer and/or the PIV Application Administrator.

The maximum number of consecutive failed Bio authentication attempts can be configured up to 15 per modality (Fingerprints, Iris, Facial) so the probability that a random attempt will succeed over a one-minute interval is:

- $15/(10^3) = 0.015$

4.2 Roles

Name	Type	Operator Type	Authentication Methods
Crypto Officer	Identity	CO	GP Secure Channel Protocol Authentication
PIV Application Administrator	Identity	Administrator	PIV Symmetric Key Authentication PIV Secret Value Authentication
User	Identity	User	PIV Symmetric Key Authentication PIV Secret Value Authentication BIO Authentication

Table 12: Roles

The module does not include a maintenance role.

The module clears previous authentications on power cycle.

© 2026 IDEMIA / atsec information security.

This document can be reproduced and distributed only whole and intact, including this copyright notice.

4.3 Approved Services

The following convention is used to specify access rights to SSPs:

- **Generate (G)**: The module generates or derives the SSP.
- **Read (R)**: The SSP is read from the module (e.g. the SSP is output).
- **Write (W)**: The SSP is updated, imported, or written to the module.
- **Execute (E)**: The module uses the SSP in performing a cryptographic operation.
- **Zeroize (Z)**: The module zeroizes the SSP.

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Reset (Show Version)	Power cycle or reset the module. Module version information returned in the card Answer to reset (ATR)	N/A	N/A	Module ATR (Contact) or ATS (Contactless) that contains configuration information	None	Unauthenticated
Select	Select an application instance.	N/A	AID of Application to Select.	Successful execution status	None	Unauthenticated
Run Self-Tests	Run all pre-operational and conditional self-tests.	N/A	'FFFFFFFFFF' Application identifier (AID) in 'Select' command's data field.	Successful execution status	AES-ECB CTR DRBG ECDSA sigGen ECDSA sigVer KAS-ECC KBKDF SP 800-108 RSA sigGen RSA sigVer SHA	Unauthenticated
Get DRBG	Retrieve random numbers.	N/A	Number of bytes or DRBG to retrieve. Up to 252 bytes (2040 bits) of DRBG	Requested number of bytes from the DRBG generator	CTR DRBG	Unauthenticated - OS-DRBG-SEED: G,E - OS-DRBG-

© 2026 IDEMIA / atsec information security.

This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
			per command			STATE: G,E
Open PIV Secure Messaging	Establish a PIV Secure Messaging (SM) communications channel.	N/A	ECC keys	Secure messaging communication channel established	AES-CBC AES-CMAC KAS-ECC	Unauthenticated - OS-DRBG-SEED: G,E - OS-DRBG-STATE: G,E - SM-C-MAC: G,E - SM-R-MAC: G,E - SM-CFRM: G,E - PIV-SM-PUB: R - PIV-SM: E - SM-ENC: E
Open Global Platform Secure Channel	Establish a Global Platform Secure Communications Channel (SC) with Mutual Authentication.	N/A	AES Keys	GP Secure Channel established	AES-CBC AES-CMAC KBKDF SP 800-108	Crypto Officer - OS-DRBG-SEED: G,E - OS-DRBG-STATE: G,E - SC-ENC: G,E - SC-C-MAC: G,E - SC-R-

© 2026 IDEMIA / atsec information security.

This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						MAC: G,E - SD-DAK: E - SD-DMK: E - SD-DEK: E
Get Data (Cleartext)	Retrieve from the Module data objects transmitted over a plaintext channel.	N/A	Tag of the Data Object to Retrieve.	Data Object Retrieved and Successful execution status	None	Unauthenticated
Get Data (SM)	Retrieve from the Module data objects transmitted with PIV Secure Messaging.	N/A	Tag of the Data Object to Retrieve for which the AC are satisfied	Data Object Retrieved and Successful execution status	None	Unauthenticated
Get Data (SC)	Retrieve from the Module data objects transmitted through a Global Platform Secure Channel.	N/A	Tag of the Data Object to Retrieve for which the AC are satisfied	Data Object Retrieved and Successful execution status	None	Unauthenticated
Get Data with Attestation using RSA (Cleartext)	Retrieve from the Module data objects together with its attestation value. Transmitted over a plaintext channel. Compliant with IG 4.1.A.	N/A	Tag of the Data Object to retrieve for which the AC are satisfied	Data Object retrieved followed by its attestation and Successful execution status.	None	Unauthenticated
Get Data with Attestation using RSA (SM)	Retrieve from the Module data objects together with its attestation value. Transmitted with PIV Secure Messaging.	N/A	Tag of the Data Object to retrieve for which the	Data Object retrieved followed by its attestation and Successful	None	Unauthenticated

© 2026 IDEMIA / atsec information security.

This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
	Compliant with IG 4.1.A.		AC are satisfied	execution status.		
Get Data with Attestation with RSA (SC)	Retrieve from the Module data objects together with its attestation value. Transmitted through a Global Platform Secure Channel. Compliant with IG 4.1.A.	N/A	Tag of the Data Object to retrieve for which the AC are satisfied	Data Object retrieved followed by its attestation and Successful execution status.	None	Unauthenticated
Get Data with Attestation Using ECDSA (Cleartext)	Retrieve from the Module data, together with its attestation value. Transmitted over a plaintext channel. Compliant with IG 4.1.A.	N/A	Tag of the Data Object to retrieve for which the AC are satisfied	Data Object retrieved followed by its attestation and Successful execution status.	None	Unauthenticated
Get Data with Attestation using ECDSA signature (SM)	Retrieve from the Module data objects together with its attestation value. Transmitted with PIV Secure Messaging. Compliant with IG 4.1.A.	N/A	Tag of the Data Object to retrieve for which the AC are satisfied	Data Object retrieved followed by its attestation and Successful execution status.	None	Unauthenticated
Get Data with Attestation using ECDSA (SC)	Retrieve from the Module data objects together with its attestation value. Transmitted through a Global Platform Secure Channel. Compliant with IG 4.1.A.	N/A	Tag of the Data Object to retrieve for which the AC are satisfied	Data Object retrieved followed by its attestation and Successful execution status.	None	Unauthenticated
Card Validation using RSA Card Authentication Key (CAK) 9E (Cleartext)	Validate the card with its asymmetric Card Authentication Key 9E, in accordance with SP800-73-4. Transmitted over a plaintext channel.	N/A	challenge data, algorithm, Key)	Authentication cryptogram computed by the module and Successful	None	Unauthenticated

© 2026 IDEMIA / atsec information security.

This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
	Compliant with IG 4.1A.			execution status		
Card Validation using RSA Card Authentication Key (CAK) 9E (SM)	Validate the card with its asymmetric Card Authentication Key 9E, in accordance with SP800-73-4. Transmitted with PIV Secure Messaging. Compliant with IG 4.1A.	N/A	Authentication material (Authentication challenge, algorithm, Key)	Authentication cryptogram computed by the module and Successful execution status	None	Unauthenticated
Card Validation using RSA Card Authentication Key (CAK) 9E (SC)	Validate the card with its asymmetric Card Authentication Key 9E, in accordance with SP800-73-4. Transmitted through a Global Platform Secure Channel. Compliant with IG 4.1A.	N/A	Authentication material (Authentication challenge, algorithm, Key)	Authentication cryptogram computed by the module and Successful execution status	None	Unauthenticated
Card Validation using ECC Card Authentication Key (CAK) 9E (Cleartext)	Validate the card with its asymmetric Card Authentication Key 9E, in accordance with SP800-73-4. Transmitted over a plaintext channel. Compliant with IG 4.1A.	N/A	challenge data, algorithm	Authentication cryptogram computed by the module and Successful execution status	None	Unauthenticated
Card Validation using ECC Card Authentication Key (CAK) 9E (SM)	Validate the card with its asymmetric Card Authentication Key 9E, in accordance with SP800-73-4. Transmitted with PIV Secure Messaging. Compliant with IG 4.1A.	N/A	Authentication material (Authentication challenge, algorithm, Key)	Authentication cryptogram computed by the module and Successful execution status	None	Unauthenticated
Card Validation using ECC Card	Validate the card with its asymmetric Card Authentication Key 9E,	N/A	Authentication material	Authentication cryptogram computed by	None	Unauthenticated

© 2026 IDEMIA / atsec information security.

This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Authentication Key (CAK) 9E (SC)	in accordance with SP800-73-4. Transmitted through a Global Platform Secure Channel. Compliant with IG 4.1A.		(Authentication challenge, algorithm, Key)	the module and Successful execution status		
Authentication with RSA PIV Authentication Key 9A (Cleartext)	Validate the card module with its PIV Authentication Key 9A, in accordance with SP800-73-4. Transmitted over a plaintext channel.	N/A	Authentication material (Authentication challenge, algorithm, Key)	Authentication cryptogram computed by the module and Successful execution status	RSA sigPrim	User - PIV-AUTH (including intermediate values): E
Authentication with RSA PIV Authentication Key 9A (SM)	Validate the card module with its PIV Authentication Key 9A, in accordance with SP800-73-4. Transmitted with PIV Secure Messaging.	N/A	Authentication material (Authentication challenge, algorithm, Key)	Authentication cryptogram computed by the module and Successful execution status	RSA sigPrim	User - PIV-AUTH (including intermediate values): E
Authentication with RSA PIV Authentication Key 9A (SC)	Authenticate with PIV Authentication Key 9A, in accordance with SP800-73-4. Transmitted through a Global Platform Secure Channel.	N/A	Authentication material (Authentication challenge, algorithm, Key)	Authentication cryptogram computed by the module and Successful execution status	RSA sigPrim	User - PIV-AUTH (including intermediate values): E
Authentication with ECC PIV Authentication Key 9A (Cleartext)	Authenticate with PIV Authentication Key 9A, in accordance with SP800-73-4. Transmitted over a plaintext channel.	N/A	Authentication material (Authentication challenge, algorithm, Key)	Authentication cryptogram computed by the module and Successful execution status	ECDSA sigGen component	User - PIV-AUTH (including intermediate

© 2026 IDEMIA / atsec information security.

This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						values): E
Authentication with ECC PIV Authentication Key 9A (SM)	Authenticate with PIV Authentication Key 9A, in accordance with SP800-73-4. Transmitted with PIV Secure Messaging.	N/A	Authentication material (Authentication challenge, algorithm, Key)	Authentication cryptogram computed by the module and Successful execution status	ECDSA sigGen component	User - PIV-AUTH (including intermediate values): E
Authentication with ECC PIV Authentication Key 9A (SC)	Authenticate with PIV Authentication Key 9A, in accordance with SP800-73-4. Transmitted through a Global Platform Secure Channel.	N/A	Authentication material (Authentication challenge, algorithm, Key)	Authentication cryptogram computed by the module and Successful execution status	ECDSA sigGen component	User - PIV-AUTH (including intermediate values): E
Digital Signature with RSA PIV Digital Signature Key 9C (Cleartext)	Sign an externally generated hash with PIV Digital Signature 9C in accordance with SP800-73-4. Transmitted over a plaintext channel.	N/A	Algorithm, Hash Value, Key	Digital Signature	RSA sigPrim	User - PIV-DS (including intermediate values): E
Digital Signature with RSA PIV Digital Signature Key 9C (SM)	Sign an externally generated hash with PIV Digital Signature 9C in accordance with SP800-73-4. Transmitted with PIV Secure Messaging.	N/A	Algorithm, Hash Value, Key	Digital Signature	RSA sigPrim	User - PIV-DS (including intermediate values): E
Digital Signature with RSA PIV	Sign an externally generated hash with PIV Digital Signature 9C in accordance with	N/A	Algorithm, Hash Value, Key	Digital Signature	RSA sigPrim	User - PIV-DS (includin

© 2026 IDEMIA / atsec information security.

This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Digital Signature Key 9C (SC)	SP800-73-4. Transmitted through a Global Platform Secure Channel.					g interme diate values): E
Digital Signature with ECC PIV Digital Signature Key 9C (Cleartext)	Sign an externally generated hash with PIV Digital Signature 9C in accordance with SP800-73-4. Transmitted over a plaintext channel.	N/A	Algorithm, Hash Value, Key	Digital Signature	ECDSA sigGen componen t	User - PIV-DS (includin g interme diate values): E
Digital Signature with ECC PIV Digital Signature Key 9C (SM)	Sign an externally generated hash with PIV Digital Signature 9C in accordance with SP800-73-4. Transmitted with PIV Secure Messaging.	N/A	Algorithm, Hash Value, Key	Digital Signature	ECDSA sigGen componen t	User - PIV-DS (includin g interme diate values): E
Digital Signature with ECC PIV Digital Signature Key 9C (SC)	Sign an externally generated hash with PIV Digital Signature 9C in accordance with SP800-73-4. Transmitted through a Global Platform Secure Channel.	N/A	Algorithm, Hash Value, Key	Digital Signature	ECDSA sigGen componen t	User - PIV-DS (includin g interme diate values): E
Full Digital Signature (RSA PSS) (Cleartext)	RSA PSS Signature with full message hashing performed within the module. Transmitted over a plaintext channel.	N/A	Algorithm, Message, Keys	Digital Signature	RSA sigGen SHA	User - DS-HASH (includin g interme diate values): E

© 2026 IDEMIA / atsec information security.

This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Full Digital Signature (RSA PSS) (SM)	RSA PSS Signature with full message hashing performed within the module. Transmitted with PIV Secure Messaging.	N/A	Algorithm, Message, Keys	Digital Signature	RSA sigGen SHA	User - DS-HASH (including intermediate values): E
Full Digital Signature (RSA PSS) (SC)	RSA PSS Signature with full message hashing performed within the module. Transmitted through a Global Platform Secure Channel.	N/A	Algorithm, Message, Keys	Digital Signature	RSA sigGen SHA	User - DS-HASH (including intermediate values): E
Full Digital Signature (ECDSA) (Cleartext)	ECDSA Signature with full message hashing performed within the module. Transmitted over a plaintext channel.	N/A	Algorithm, Message, Keys	Digital Signature	ECDSA sigGen SHA	User - DS-HASH (including intermediate values): E
Full Digital Signature (ECDSA) (SM)	ECDSA Signature with full message hashing performed within the module. Transmitted with PIV Secure Messaging.	N/A	Algorithm, Message, Keys	Digital Signature	ECDSA sigGen SHA	User - DS-HASH (including intermediate values): E
Full Digital Signature (ECDSA) (SC)	ECDSA Signature with full message hashing performed within the module. Transmitted through a Global	N/A	Algorithm, Message, Keys	Digital Signature	ECDSA sigGen SHA	User - DS-HASH (including interme

© 2026 IDEMIA / atsec information security.

This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
	Platform Secure Channel.					diate values): E
System Key Services with PIV Key Management Keys (RSA) (Cleartext)	Decrypt a key or generate a shared secret using the module Key Management Keys, in accordance with SP800-73-4. Transmitted over a plaintext channel. Key decryption is the use of SP800-56B Section 7.1.2 RSADP key decryption primitive.	N/A	Algorithm, RSA Wrapped System Key	Unwrapped key. The unwrapped key is for the outside system and is not used by the module.	RSA Decryption Primitive (CVL)	User - PIV-KMK (including intermediate values): E
System Key Services with PIV Key Management Keys (RSA) (SM)	Decrypt a key or generate a shared secret using the module Key Management Keys, in accordance with SP800-73-4. Transmitted with PIV Secure Messaging. Key decryption is the use of SP800-56B Section 7.1.2 RSADP key decryption primitive.	N/A	Algorithm, RSA Wrapped System Key	Unwrapped key. The unwrapped key is for the outside system and is not used by the module.	RSA Decryption Primitive (CVL)	User - PIV-KMK (including intermediate values): E
System Key Services with PIV Key Management Keys (RSA) (SC)	Decrypt a key or generate a shared secret using the module Key Management Keys, in accordance with SP800-73-4. Transmitted through a Global Platform Secure Channel. Key decryption is the use of SP800-56B Section	N/A	Algorithm, RSA Wrapped System Key	Unwrapped key. The unwrapped key is for the outside system and is not used by the module.	RSA Decryption Primitive (CVL)	User - PIV-KMK (including intermediate values): E

© 2026 IDEMIA / atsec information security.

This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
	7.1.2 RSADP key decryption primitive.					
System Key Services with PIV Key Management Keys (ECDH) (Cleartext)	Decrypt a key or generate a shared secret using the module Key Management Keys, in accordance with SP800-73-4. Transmitted over a plaintext channel. Shared secret generation is the use of SP800-56A Section 5.7.1.2.	N/A	Algorithm, ECC Public key	Unwrapped Shared Secret. The unwrapped shared secret is for the outside system and is not used by the module.	KAS-ECC CDH Component	User - PIV-KMK (including intermediate values): E
System Key Services with PIV Key Management Keys (ECDH) (SM)	Decrypt a key or generate a shared secret using the module Key Management Keys, in accordance with SP800-73-4. Transmitted with PIV Secure Messaging. Shared secret generation is the use of SP800-56A Section 5.7.1.2.	N/A	Algorithm, ECC Public key	Unwrapped Shared Secret. The unwrapped shared secret is for the outside system and is not used by the module.	KAS-ECC CDH Component	User - PIV-KMK (including intermediate values): E
System Key Services with PIV Key Management Keys (ECDH) (SC)	Decrypt a key or generate a shared secret using the module Key Management Keys, in accordance with SP800-73-4. Transmitted through a Global Platform Secure Channel. Shared secret generation is the use of SP800-56A Section 5.7.1.2.	N/A	Algorithm, ECC Public key	Unwrapped Shared Secret. The unwrapped shared secret is for the outside system and is not used by the module.	KAS-ECC CDH Component	User - PIV-KMK (including intermediate values): E

© 2026 IDEMIA / atsec information security.

This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Card Validation using Symmetric Card Authentication Key (Cleartext)	Authenticate the module with its Symmetric Card Authentication Key, in accordance with SP800-73-4. Transmitted over a plaintext channel. Compliant with IG 4.1A.	N/A	Authentication material (Authentication challenge, algorithm, Key)	Authentication cryptogram computed by the module and Successful execution status	None	Unauthenticated
Card Validation using Symmetric Card Authentication Key (SM)	Authenticate the module with its Symmetric Card Authentication Key, in accordance with SP800-73-4. Transmitted with PIV Secure Messaging. Compliant with IG 4.1A.	N/A	Authentication material (Authentication challenge, algorithm, Key)	Authentication cryptogram computed by the module and Successful execution status	None	Unauthenticated
Card Validation using Symmetric Card Authentication Key (SC)	Authenticate the module with its Symmetric Card Authentication Key, in accordance with SP800-73-4. Transmitted through a Global Platform Secure Channel. Compliant with IG 4.1A.	N/A	Authentication material (Authentication challenge, algorithm, Key)	Authentication cryptogram computed by the module and Successful execution status	None	Unauthenticated
External Authentication with PIV Admin Key (Cleartext)	External Authentication of AA role to the module using PIV Admin Key in accordance with SP800-73-4. Transmitted over a plaintext channel.	N/A	Authentication material (Authentication Cryptogram, algorithm, Key)	Authentication Challenge,Successful execution status	AES-ECB	PIV Application Administrator - ADMIN_KEY: E
External Authentication with	External Authentication of AA role to the	N/A	Authentication	Authentication Challenge,Succ	AES-ECB	PIV Applicati

© 2026 IDEMIA / atsec information security.

This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
PIV Admin Key (SM)	module using PIV Admin Key in accordance with SP800-73-4. Transmitted with PIV Secure Messaging.		material (Authentication Cryptogram, algorithm, Key)	essful execution status		on Administrator - ADMIN_KEY: E
External Authentication with PIV Admin Key (SC)	External Authentication of AA role to the module using PIV Admin Key in accordance with SP800-73-4. Transmitted through a Global Platform Secure Channel.	N/A	Authentication material (Authentication Cryptogram, algorithm, Key)	Authentication Challenge,Successful execution status	AES-ECB	PIV Application Administrator - ADMIN_KEY: E
Mutual Authentication with PIV Admin Key (Cleartext)	Mutual Authentication of AA role to the module using PIV Admin Key in accordance with SP800-73-4. Transmitted over a plaintext channel.	N/A	Authentication material (Authentication Cryptogram, algorithm, Key, Authentication challenge)	Authentication cryptogram computed by the module, Authentication Challenge,Successful execution status	AES-ECB	PIV Application Administrator - ADMIN_KEY: E
Mutual Authentication with PIV Admin Key (SM)	Mutual Authentication of AA role to the module using PIV Admin Key in accordance with SP800-73-4. Transmitted with PIV Secure Messaging.	N/A	Authentication material (Authentication Cryptogram, algorithm, Key, Authentication challenge)	Authentication cryptogram computed by the module, Authentication Challenge,Successful execution status	AES-ECB	PIV Application Administrator - ADMIN_KEY: E
Mutual Authentication with	Mutual Authentication of AA role to the module using PIV	N/A	Authentication material	Authentication cryptogram computed by	AES-ECB	PIV Application

© 2026 IDEMIA / atsec information security.

This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
PIV Admin Key (SC)	Admin Key in accordance with SP800-73-4. Transmitted through a Global Platform Secure Channel.		(Authentication Cryptogram, algorithm, Key, Authentication challenge)	the module, Authentication Challenge,Successful execution status		Administrator - ADMIN_KEY: E
Mutual Authentication with Mutual Authentication Key (Cleartext)	Mutual authentication between the module and an Administrator Key. Transmitted over a plaintext channel.	N/A	Authentication Cryptogram, algorithm, Admin Key)	Authentication cryptogram computed by the module, Authentication Challenge,Successful execution status	AES-ECB	PIV Application Administrator - MUTUAL-AUTH: E
Mutual Authentication with Mutual Authentication Key (SM)	Mutual authentication between the module and an Administrator Key. Transmitted with PIV Secure Messaging.	N/A	Authentication Cryptogram, algorithm, Admin Key)	Authentication cryptogram computed by the module, Authentication Challenge,Successful execution status	AES-ECB	PIV Application Administrator - MUTUAL-AUTH: E
Mutual Authentication with Mutual Authentication Key (SC)	Mutual authentication between the module and an Administrator Key. Transmitted through a Global Platform Secure Channel.	N/A	Authentication Cryptogram, algorithm, Admin Key)	Authentication cryptogram computed by the module, Authentication Challenge,Successful execution status	AES-ECB	PIV Application Administrator - MUTUAL-AUTH: E
Global Platform Lock / Unlock	Temporarily lock & unlock the full module or one of its applications using	N/A	Global Platform card life cycle	Successful execution status	AES-CBC AES-CMAC	Crypto Officer - SC-ENC: E

© 2026 IDEMIA / atsec information security.

This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
	Global Platform card life cycle status.		status to set, and AID of the application			- SC-C-MAC: E - SC-R-MAC: E
Module Termination	Set the card life cycle status to TERMINATED. All the CSPs are zeroized when the life cycle status is set to TERMINATED	N/A	N/A	Successful execution status	AES-CBC AES-CMAC	Crypto Officer - SC-ENC: E,Z - SC-C-MAC: E,Z - SC-R-MAC: E,Z - OS-DRBG-SEED: Z - OS-DRBG-STATE: Z - SD-DAK: Z - SD-DMK: Z - SD-DEK: Z - DAP-AES: Z - PIV-SM: Z - SM-ENC: Z - SM-C-MAC: Z - SM-R-MAC: Z - SM-CFRM: Z - PIN: Z - OCC-Fingerpr

© 2026 IDEMIA / atsec information security.

This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						ints: Z - OCC-Facial: Z - OCC-Iris: Z - PUK: Z - ADMIN_PIN: Z - ADMIN_KEY: Z - PIV-AUTH (including intermediate values): Z - PIV-DS (including intermediate values): Z - PIV-KMK (including intermediate values): Z - MUTUAL-AUTH: Z - DS-HASH (including interme

© 2026 IDEMIA / atsec information security.

This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						diate values): Z - SAM-CMAC: Z - SAM-KDF: Z - SAM-KDF-ENC: Z - HOTP: Z - TOTP-SHA1: Z - TOTP-SHA256: Z - TOTP-SHA512: Z - DAP-PUB (including intermediate values): Z - PIV-SM-PUB: Z - PIV-AUTH-PUB (including intermediate values): Z - PIV-DS-PUB (including interme

© 2026 IDEMIA / atsec information security.

This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						diate values): Z - PIV-KMK-PUB (including intermediate values): Z - DS-HASH-PUB (including intermediate values): Z - FIDO-UV-PIN: Z - CTAP2 ECDH-PRIV: Z - CTAP2 ECDH-PUB: Z - CTAP2 Shared Secret: Z - CTAP2 HMAC key: Z - CTAP2 AES key: Z - pinUvAuthToken: Z - Attestati

© 2026 IDEMIA / atsec information security.

This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						on Private Key: Z - Enterprise Attestation Private Key: Z - Discoverable Credential Private Key: Z - Non-Discoverable Credential Private Key: Z - Attestation Public Key: Z - Enterprise Attestation Public Key: Z - Discoverable Credential Public Key: Z - Non-Discoverable Credenti

© 2026 IDEMIA / atsec information security.

This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						al Public Key: Z - Wrapping ENC Key: Z - Wrapping MAC Key: Z
Load FW with RSA DAP	Load and install application packages (FW).	N/A	Signed Packages (FW)	Successful execution status	AES-CBC AES-CMAC RSA sigVer	Crypto Officer - DAP-PUB (including intermediate values): E
Load FW with AES DAP	Load and install application packages (FW).	N/A	Signed Packages (FW)	Successful execution status	AES-CBC AES-CMAC	Crypto Officer - DAP-AES: E
Manage SD Keys and PIV Global Reference Data	Update SD keys and reset PIV Global Reference Data (PINs & BIO with an ID in the Global ID Range).	N/A	SD keys or PIV Global Reference Data	Successful execution status	AES-CBC AES-CMAC KTS (AES + CMAC) key wrapping/ unwrapping	Crypto Officer - DAP-PUB (including intermediate values): W,E - SC-ENC: E - SC-C-MAC: E - SC-R-MAC: E - SD-DAK: W - SD-DMK: W

© 2026 IDEMIA / atsec information security.

This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- SD-DEK: W - DAP-AES: W - PIN: W - PUK: W - ADMIN_PIN: W - OCC-Fingerprints: W - OCC-Facial: W - OCC-Iris: W
Manage SD Data	Create or update Security Domain (SD) data.	N/A	SD Data	Successful execution status	AES-CBC AES-CMAC	Crypto Officer - SD-DEK: E - SC-ENC: E - SC-C-MAC: E - SC-R-MAC: E
Show Status	Retrieve the identification and status of all applications present in the module	N/A	Level of details to retrieve	Requested application status and Successful execution status	AES-CBC AES-CMAC	Crypto Officer - SC-ENC: E - SC-C-MAC: E - SC-R-MAC: E
Global Platform DELETE APPLICATION	Remove an application and all its data and keys from the module.	N/A	AID of the application to remove	Successful execution status	AES-CBC AES-CMAC	Crypto Officer - PIN: Z - OCC-Fingerprints: Z - OCC-Facial: Z

© 2026 IDEMIA / atsec information security.

This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- OCC-Iris: Z - PUK: Z - ADMIN_PIN: Z - ADMIN_KEY: Z - PIV-AUTH (including intermediate values): Z - PIV-DS (including intermediate values): Z - PIV-KMK (including intermediate values): Z - MUTUAL-AUTH: Z - DS-HASH (including intermediate values): Z

© 2026 IDEMIA / atsec information security.

This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- SAM-CMAC: Z - SM-R-MAC: Z - SM-CFRM: Z - HOTP: Z - TOTP-SHA1: Z - TOTP-SHA256: Z - TOTP-SHA512: Z - DAP-PUB (including intermediate values): Z - PIV-SM-PUB: Z - PIV-AUTH-PUB (including intermediate values): Z - PIV-DS-PUB (including intermediate values): Z

© 2026 IDEMIA / atsec information security.

This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- PIV-KMK-PUB (including intermediate values): Z - DS-HASH-PUB (including intermediate values): Z - FIDO-UV-PIN: Z - CTAP2 ECDH-PRIV: Z - CTAP2 ECDH-PUB: Z - CTAP2 Shared Secret: Z - CTAP2 HMAC key: Z - CTAP2 AES key: Z - pinUvAuthToken: Z - Attestation Private Key: Z

© 2026 IDEMIA / atsec information security.

This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- Enterprise Attestation Private Key: Z - Discoverable Credential Private Key: Z - Non-Discoverable Credential Private Key: Z - Attestation Public Key: Z - Enterprise Attestation Public Key: Z - Discoverable Credential Public Key: Z - Non-Discoverable Credential Public Key: Z -

© 2026 IDEMIA / atsec information security.

This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Wrapping ENC Key: Z - Wrapping MAC Key: Z
Personalize PIV Data (Cleartext)	Write data into the PIV application. Transmitted over a plaintext channel.	N/A	Data Object or Elementary file to update.	Successful execution status	None	PIV Application Administrator - SC-ENC: Z - SC-C-MAC: Z - SC-R-MAC: Z
Personalize PIV Data (SM)	Write data into the PIV application. Transmitted with PIV Secure Messaging.	N/A	Data Object or Elementary file to update.	Successful execution status	None	PIV Application Administrator - SM-ENC: E,Z - SM-C-MAC: E,Z - SM-R-MAC: E,Z
Personalize PIV Data (SC)	Write data into the PIV application. Transmitted through a Global Platform Secure Channel.	N/A	Data Object or Elementary file to update.	Successful execution status	None	PIV Application Administrator - SD-DEK: E - SC-ENC: E - SC-C-MAC: E

© 2026 IDEMIA / atsec information security.

This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- SC-R-MAC: E
Manage PIV Local Reference Data (Cleartext)	Personalize authentication datum or local biometric data for OCC (i.e. with an ID in the local ID range). Transmitted over a plaintext channel.	N/A	Local authentication datum or biometric data for OCC	Successful execution status	AES-CBC AES-CMAC	Crypto Officer - SC-ENC: Z - SC-C-MAC: Z - SC-R-MAC: Z - PIN: W - PUK: W - ADMIN_PIN: W - OCC-Fingerprints: W,Z
Manage PIV Local Reference Data (SM)	Personalize authentication datum or local biometric data for OCC (i.e. with an ID in the local ID range). Transmitted with PIV Secure Messaging.	N/A	Local authentication datum or biometric data for OCC	Successful execution status	AES-CBC AES-CMAC	Crypto Officer - SM-ENC: E,Z - SM-C-MAC: E,Z - SM-R-MAC: E,Z - PIN: W - PUK: W - ADMIN_PIN: W - OCC-Fingerprints: W,Z

© 2026 IDEMIA / atsec information security.

This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Manage PIV Local Reference Data (SC)	Personalize authentication datum or local biometric data for OCC (i.e. with an ID in the local ID range). Transmitted through a Global Platform Secure Channel.	N/A	Local authentication datum or biometric data for OCC	Successful execution status	AES-CBC AES-CMAC	Crypto Officer - SD-DEK: E - SC-ENC: E - SC-C-MAC: E - SC-R-MAC: E - PIN: W - PUK: W - ADMIN_PIN: W - OCC-Fingerprints: W,Z
On-Board-Key-Generation (CKG) - RSA (Cleartext)	Generate Asymmetric Key pair (RSA) inside the module, and export the public key value. Not supported for PIV Key Management Keys. Transmitted over a plaintext channel.	N/A	CKG parameters (algorithm, key size, Key ID)	Public Key generated, Successful execution status	RSA keyGen RSA sigPrim RSA sigVer	PIV Application Administrator - SC-ENC: Z - SC-C-MAC: Z - SC-R-MAC: Z - PIV-AUTH (including intermediate values): G - PIV-AUTH-PUB (including interme

© 2026 IDEMIA / atsec information security.

This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						diate values): G - PIV-DS (including intermediate values): G - PIV-DS-PUB (including intermediate values): G - PIV-SM: G - PIV-SM-PUB: G - DS-HASH (including intermediate values): G - DS-HASH-PUB (including intermediate values): G
On-Board-Key-Generation (CKG) - RSA (SM)	Generate Asymmetric Key pair (RSA) inside the module, and export the public key value.	N/A	CKG parameters (algorithm,	Public Key generated, Successful	RSA keyGen RSA sigPrim	PIV Application Administ

© 2026 IDEMIA / atsec information security.

This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
	Not supported for PIV Key Management Keys. Transmitted with PIV Secure Messaging.		key size, Key ID)	execution status	RSA sigVer	rator - SM-ENC: E,Z - SM-C-MAC: E,Z - SM-R-MAC: E,Z - PIV-AUTH (including intermediate values): G - PIV-AUTH-PUB (including intermediate values): G - PIV-DS (including intermediate values): G - PIV-DS-PUB (including intermediate values): G - PIV-SM: G - PIV-

© 2026 IDEMIA / atsec information security.

This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						SM-PUB: G - DS-HASH (including intermediate values): G - DS-HASH-PUB (including intermediate values): G
On-Board-Key-Generation (CKG) - RSA (SC)	Generate Asymmetric Key pair (RSA) inside the module, and export the public key value. Not supported for PIV Key Management Keys. Transmitted through a Global Platform Secure Channel.	N/A	CKG parameters (algorithm, key size, Key ID)	Public Key generated, Successful execution status	RSA keyGen RSA sigPrim RSA sigVer	PIV Application Administrator - SD-DEK: E - SC-ENC: E - SC-C-MAC: E - SC-R-MAC: E - PIV-AUTH (including intermediate values): G - PIV-AUTH-PUB (including

© 2026 IDEMIA / atsec information security.

This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						intermediate values): G - PIV-DS (including intermediate values): G - PIV-DS-PUB (including intermediate values): G - PIV-SM: G - PIV-SM-PUB: G - DS-HASH (including intermediate values): G - DS-HASH-PUB (including intermediate values): G
On-Board-Key-Generation (CKG) - ECC (Cleartext)	Generate Asymmetric Key pair (ECC) inside the module, and export	N/A	CKG parameters	Public Key generated, Successful	ECDSA keyGen ECDSA	PIV Application

© 2026 IDEMIA / atsec information security.

This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
	the public key value. Not supported for PIV Key Management Keys. Transmitted over a plaintext channel.		(algorithm, key size, Key ID)	execution status	sigGen component ECDSA sigVer ECDSA keyVer	Administrator - SC-ENC: Z - SC-C-MAC: Z - SC-R-MAC: Z - PIV-AUTH (including intermediate values): G - PIV-AUTH-PUB (including intermediate values): G - PIV-DS (including intermediate values): G - PIV-DS-PUB (including intermediate values): G - PIV-SM: G - PIV-SM-PUB: G

© 2026 IDEMIA / atsec information security.

This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- DS-HASH (including intermediate values): G - DS-HASH-PUB (including intermediate values): G
On-Board-Key-Generation (CKG) - ECC (SM)	Generate Asymmetric Key pair (ECC) inside the module, and export the public key value. Not supported for PIV Key Management Keys. Transmitted with PIV Secure Messaging.	N/A	CKG parameters (algorithm, key size, Key ID)	Public Key generated, Successful execution status	ECDSA keyGen ECDSA sigGen component ECDSA sigVer ECDSA keyVer	PIV Application Administrator - SM-ENC: E,Z - SM-C-MAC: E,Z - SM-R-MAC: E,Z - PIV-AUTH (including intermediate values): G - PIV-AUTH-PUB (including interme

© 2026 IDEMIA / atsec information security.

This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						diate values): G - PIV-DS (including intermediate values): G - PIV-DS-PUB (including intermediate values): G - PIV-SM: G - PIV-SM-PUB: G - DS-HASH (including intermediate values): G - DS-HASH-PUB (including intermediate values): G
On-Board-Key-Generation (CKG) - ECC (SC)	Generate Asymmetric Key pair (ECC) inside the module, and export the public key value.	N/A	CKG parameters (algorithm,	Public Key generated, Successful	ECDSA keyGen ECDSA sigGen	PIV Application Administ

© 2026 IDEMIA / atsec information security.

This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
	Not supported for PIV Key Management Keys. Transmitted through a Global Platform Secure Channel.		key size, Key ID)	execution status	component ECDSA sigVer ECDSA keyVer	rator - SD-DEK: E - SC-ENC: E - SC-C-MAC: E - SC-R-MAC: E - PIV-AUTH (including intermediate values): G - PIV-AUTH-PUB (including intermediate values): G - PIV-DS (including intermediate values): G - PIV-DS-PUB (including intermediate values): G - PIV-SM: G - PIV-SM-

© 2026 IDEMIA / atsec information security.

This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						PUB: G - DS-HASH (including intermediate values): G - DS-HASH-PUB (including intermediate values): G
PIV Put Key (SM)	Secure inject PIV Application keys. Transmitted with PIV Secure Messaging.	N/A	Algorithm & Encrypted Key value	Successful execution status	AES-CBC AES-CMAC KTS (AES + CMAC) key wrapping/ unwrapping	Crypto Officer - SM-ENC: E,Z - SM-C-MAC: E,Z - SM-R-MAC: E,Z - ADMIN_KEY: W,Z - PIV-AUTH (including intermediate values): W,Z - PIV-AUTH-PUB (includin

© 2026 IDEMIA / atsec information security.

This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						g intermediate values): W,Z - PIV-DS (including intermediate values): W,Z - PIV-DS-PUB (including intermediate values): W,Z - PIV-KMK (including intermediate values): W,Z - PIV-KMK-PUB (including intermediate values): W,Z - PIV-SM: W,Z - PIV-SM-PUB: W,Z -

© 2026 IDEMIA / atsec information security.

This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						MUTUAL-AUTH: W,Z - DS-HASH (including intermediate values): W,Z - DS-HASH-PUB (including intermediate values): W,Z - SAM-CMAC: W,Z - SAM-KDF: W,Z - SAM-KDF-ENC: W,Z - HOTP: W,Z - TOTP-SHA1: W,Z - TOTP-SHA256: W,Z - TOTP-SHA512: W,Z PIV Application Administ

© 2026 IDEMIA / atsec information security.

This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						rator - SM-ENC: E,Z - SM-C-MAC: E,Z - SM-R-MAC: E,Z - ADMIN_KEY: W,Z - PIV-AUTH (including intermediate values): W,Z - PIV-AUTH-PUB (including intermediate values): W,Z - PIV-DS (including intermediate values): W,Z - PIV-DS-PUB (including intermediate values):

© 2026 IDEMIA / atsec information security.

This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						W,Z - PIV-KMK (including intermediate values): W,Z - PIV-KMK-PUB (including intermediate values): W,Z - PIV-SM: W,Z - PIV-SM-PUB: W,Z - MUTUAL-AUTH: W,Z - DS-HASH (including intermediate values): W,Z - DS-HASH-PUB (including intermediate values):

© 2026 IDEMIA / atsec information security.

This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						W,Z - SAM-CMAC: W,Z - SAM-KDF: W,Z - SAM-KDF-ENC: W,Z - HOTP: W,Z - TOTP-SHA1: W,Z - TOTP-SHA256: W,Z - TOTP-SHA512: W,Z
PIV Put Key (SC)	Secure inject PIV Application keys. Transmitted through a Global Platform Secure Channel.	N/A	Algorithm & Encrypted Key value	Successful execution status	AES-ECB AES-CMAC KTS (AES + CMAC) key wrapping/ unwrapping	Crypto Officer - SD-DEK: E - SC-ENC: E - SC-C-MAC: E - SC-R-MAC: E - ADMIN_KEY: W,Z - PIV-AUTH (including intermediate values): W,Z - PIV-

© 2026 IDEMIA / atsec information security.

This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						AUTH-PUB (including intermediate values): W,Z - PIV-DS (including intermediate values): W,Z - PIV-DS-PUB (including intermediate values): W,Z - PIV-KMK (including intermediate values): W,Z - PIV-KMK-PUB (including intermediate values): W,Z - PIV-SM: W,Z - PIV-SM-

© 2026 IDEMIA / atsec information security.

This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						PUB: W,Z - MUTUAL-AUTH: W,Z - DS-HASH (including intermediate values): W,Z - DS-HASH-PUB (including intermediate values): W,Z - SAM-CMAC: W,Z - SAM-KDF: W,Z - SAM-KDF-ENC: W,Z - HOTP: W,Z - TOTP-SHA1: W,Z - TOTP-SHA256: W,Z - TOTP-SHA512: W,Z PIV

© 2026 IDEMIA / atsec information security.

This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Application Administrator - SD-DEK: E - SC-ENC: E - SC-C-MAC: E - SC-R-MAC: E - ADMIN_KEY: W,Z - PIV-AUTH (including intermediate values): W,Z - PIV-AUTH-PUB (including intermediate values): W,Z - PIV-DS (including intermediate values): W,Z - PIV-DS-PUB (including interme

© 2026 IDEMIA / atsec information security.

This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						diate values): W,Z - PIV-KMK (including intermediate values): W,Z - PIV-KMK-PUB (including intermediate values): W,Z - PIV-SM: W,Z - PIV-SM-PUB: W,Z - MUTUAL-AUTH: W,Z - DS-HASH (including intermediate values): W,Z - DS-HASH-PUB (including interme

© 2026 IDEMIA / atsec information security.

This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						diate values): W,Z - SAM-CMAC: W,Z - SAM-KDF: W,Z - SAM-KDF-ENC: W,Z - HOTP: W,Z - TOTP-SHA1: W,Z - TOTP-SHA256: W,Z - TOTP-SHA512: W,Z
Verify Reference Data (Cleartext)	Send authentication datum (PINs or BIO) for verification. Transmitted over an unprotected channel.	N/A	Authentication Data	Successful execution status	None	PIV Application Administrator - PUK: E - ADMIN_PIN: E User - PIN: E - OCC-Fingerprints: E - OCC-Facial: E - OCC-Iris: E

© 2026 IDEMIA / atsec information security.

This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Verify Reference Data (SM)	Send authentication datum (PINs or BIO) for verification. Transmitted with a PIV Secure Messaging.	N/A	Authentication Data	Successful execution status	None	PIV Application Administrator - PUK: E - ADMIN_PIN: E User - PIN: E - OCC-Fingerprints: E - OCC-Facial: E - OCC-Iris: E
Verify Reference Data (SC)	Send authentication datum (PINs or BIO) for verification. Transmitted through a Global Platform Secure Channel.	N/A	Authentication Data	Successful execution status	None	PIV Application Administrator - PUK: E - ADMIN_PIN: E User - PIN: E - OCC-Fingerprints: E - OCC-Facial: E - OCC-Iris: E
Un-verify Reference Data (Cleartext)	Clear the verification status of previously verified reference data (PINs or BIO).	N/A	Authentication Data	Successful execution status	None	PIV Application Administ

© 2026 IDEMIA / atsec information security.

This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
	Following execution of this service, a new Verify Reference Data shall be called to set its status to "verified" and unlock the associated Access Condition (AC). Transmitted over an unprotected channel.					rator - PUK: E - ADMIN_PIN: E User - PIN: E - OCC-Fingerprints: E - OCC-Facial: E - OCC-Iris: E
Un-verify Reference Data (SM)	Clear the verification status of previously verified reference data (PINs or BIO). Following execution of this service, a new Verify Reference Data shall be called to set its status to "verified" and unlock the associated Access Condition (AC). Transmitted with a PIV Secure Messaging.	N/A	Authentication Data	Successful execution status	None	PIV Application Administrator - PUK: E - ADMIN_PIN: E User - PIN: E - OCC-Fingerprints: E - OCC-Facial: E - OCC-Iris: E
Un-verify Reference Data (SC)	Clear the verification status of previously verified reference data (PINs or BIO). Following execution of this service, a new Verify Reference Data shall be called to set its status to "verified"	N/A	Authentication Data	Successful execution status	None	PIV Application Administrator - PUK: E - ADMIN_

© 2026 IDEMIA / atsec information security.

This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
	and unlock the associated Access Condition (AC). Transmitted through a Global Platform Secure Channel.					PIN: E User - PIN: E - OCC-Fingerprints: E - OCC-Facial: E - OCC-Iris: E
SAM computation (SM)	Use the PIV card as a SAM to compute CMAC, KDF or authentication cryptogram to unlock a target card. Transmitted with PIV Secure Messaging.	N/A	Diversification data	AES-CMAC value, or KDF or Authentication Cryptogram depending on the SAM Key being used (SAM-CMAC, SAM-KDF, SAM-KDF-ENC)	AES-CBC AES-CMAC	User - SAM-CMAC: E - SAM-KDF: E - SAM-KDF-ENC: E
SAM computation (SC)	Use the PIV card as a SAM to compute CMAC, KDF or authentication cryptogram to unlock a target card. Transmitted through a Global Platform Secure Channel.	N/A	Diversification data	AES-CMAC value, or KDF or Authentication Cryptogram depending on the SAM Key being used (SAM-CMAC, SAM-KDF, SAM-KDF-ENC)	AES-CBC AES-CMAC	User - SAM-CMAC: E - SAM-KDF: E - SAM-KDF-ENC: E
One-Time-Password Generation (HOTP)	Compute an HMAC-Based One Time Password (HOTP)	N/A	N/A for HOTP (the counter is managed by the module)	HMAC-Based One-time Password (HOTP) value computed as per RFC 4226	HMAC	User - HOTP: E

© 2026 IDEMIA / atsec information security.

This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
One-Time-Password Generation (TOTP)	Compute a One Time Password (TOTP)	N/A	time stamp	Time-based One-time Password (TOTP) algorithm specified in RFC 6238	HMAC	User - TOTP-SHA1: E - TOTP-SHA256: E - TOTP-SHA512: E
CTAP MakeCredential	Request generation of a new authenticator credential	N/A	Client data hash, relying party info, user, key parameters, exclude list, attestation formats, extensions	attestation statement format identifier, authData, attestation statement, credential flags, extension data	AES-CBC CTR DRBG ECDSA keyGen ECDSA keyVer ECDSA sigGen HMAC KTS (AES + HMAC) key wrapping/ unwrapping	Crypto Officer - Attestation Private Key: G,E - Enterprise Attestation Private Key: G,E - Discoverable Credential Private Key: G,E - Non-Discoverable Credential Private Key: G,E - Attestation Public

© 2026 IDEMIA / atsec information security.

This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Key: G,R - Enterprise Attestation Public Key: G,R - Discoverable Credential Public Key: G,R - Non-Discoverable Credential Public Key: G,R - Wrapping ENC Key: E - Wrapping MAC Key: E
CTAP GetAssertion	Request cryptographic proof of user authentication as well as user consent to a given transaction, using a previously generated credential that is bound to the authenticator and relying party identifier	N/A	Client data hash, relying party info, allowList, extensions, number of credentials	PublicKeyCredentialDescriptor, authData, signature, user account information,	AES-CBC ECDSA sigGen HMAC KAS-ECC (FIDO)	Crypto Officer - Attestation Private Key: E - Enterprise Attestation Private

© 2026 IDEMIA / atsec information security.

This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Key: E - Discoverable Credential Private Key: E - Non-Discoverable Credential Private Key: E - FIDO-UV-PIN: W,E - CTAP2 ECDH-PRIV: E - CTAP2 ECDH-PUB: W,E - CTAP2 Shared Secret: G,E,Z - CTAP2 HMAC key: G,E - CTAP2 AES key: G,E
CTAP GetNextAssertion	Used to obtain the next per-credential signature for a given GetAssertion request	N/A	Client data hash, relying party info, allowList, extensions, number of credentials	PublicKeyCredentialDescriptor, authData, signature, user account information,	AES-CBC ECDSA sigGen HMAC KAS-ECC (FIDO)	Crypto Officer - Attestation Private Key: E - Enterprise

© 2026 IDEMIA / atsec information security.

This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Attestation Private Key: E - Discoverable Credential Private Key: E - Non-Discoverable Credential Private Key: E - FIDO-UV-PIN: W,E - CTAP2 ECDH-PRIV: E - CTAP2 ECDH-PUB: W,E - CTAP2 Shared Secret: G,E,Z - CTAP2 HMAC key: G,E - CTAP2 AES key: G,E
CTAP ClientPIN	Used to import encrypted PINs to the authenticator	N/A	AuthProtocol, subCommand, platforms key agreement	public key agreement key, AuthToken, retry count, power cycle state	AES-CBC CTR DRBG HMAC KAS-ECC (FIDO)	Crypto Officer - CTAP2 AES key: G,E - CTAP2 HMAC

© 2026 IDEMIA / atsec information security.

This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
			key, AuthParam, encrypted PIN, encrypted pin hash, permissions, relying party ID			key: G,E - CTAP2 Shared Secret: G,E,Z - CTAP2 ECDH-PRIV: E - CTAP2 ECDH-PUB: W,E - FIDO-UV-PIN: W,E,Z - pinUvAuthToken: G,E
CTAP GetInfo	Used to report a list of supported protocol versions and extensions, the AAGUID, and other aspects of its overall capabilities.	N/A	N/A	Versions list , extensions list, AAGUID, options, max msg size, AuthProtocols, max number of credentials, algorithms, min PIN length, firmware version, remaining number of discoverable credentials that can be stored	None	Unauthenticated
CTAP Reset	Used to return the authentication to the factory default state.	N/A	N/A	Successful execution status	None	Crypto Officer - FIDO-UV-PIN: Z - CTAP2 ECDH-PRIV: Z - CTAP2

© 2026 IDEMIA / atsec information security.

This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						ECDH-PUB: Z - CTAP2 Shared Secret: Z - CTAP2 HMAC key: Z - CTAP2 AES key: Z - pinUvAuthToken: Z - Attestation Private Key: Z - Enterprise Attestation Private Key: Z - Discoverable Credential Private Key: Z - Non-Discoverable Credential Private Key: Z - Attestation Public

© 2026 IDEMIA / atsec information security.

This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Key: Z - Enterprise Attestation Public Key: Z - Discoverable Credential Public Key: Z - Non-Discoverable Credential Public Key: Z - Wrapping ENC Key: Z - Wrapping MAC Key: Z
CTAP CredentialManagement	Used to manage discoverable credentials on the authenticator.	N/A	Sub command, sub command parameters, AuthParameter	Number of credentials, max number of credentials, relying party information, user information, credential public key, credential protection policy	HMAC	Crypto Officer - pinUvAuthToken: E
CTAP Selection	Signal to the authenticator to request user presence	N/A	N/A	Successful execution status	None	Unauthenticated

© 2026 IDEMIA / atsec information security.

This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
CTAP Config	Used to configure various authenticator features through the use of its subcommands	N/A	subCommand, subCommandParams, AuthProtocol, AuthParams	Successful execution status	HMAC	Crypto Officer - pinUvAuthToken: E
CTAP VendorSpecificGetMacPinUvAuthToken	Used to retrieve MAC of the encrypted pinUvAuthToken which is returned as response message of command authenticatorClientPIN sub command getPinToken, or sub command getPinUvAuthTokenUsingPinWithPermissions	N/A	N/A	MAC of encrypted pinUvAuthToken	HMAC	Crypto Officer - CTAP2 HMAC key: E

Table 13: Approved Services

The module supports unauthenticated services which perform cryptographic operations yet do not claim any security provided by the module but instead serves to identify the module to an external entity for attestation services. Item '1b' in IG 4.1.A "Additional Comments" section provides a list of rationales for which exemption can be claimed. These are:

a) the referenced algorithms and services do not create, disclose, modify, substitute, access, or make use of the module’s CSPs, and PSPs are not modified or substituted; or
b) that the referenced algorithms and services do not affect the security of the module, or the security of the information being protected by the module.

The module implements PIV card validation and attestation services that use symmetric keys and asymmetric private keys purely to provide the module's cryptographic identity to an external entity. The use of cryptographic challenge-response schemes with symmetric keys use of asymmetric signature verification schemes to validate private keys embedded within the module are not claimed to provide protection of data but rather only serve to confirm the module's identity to an external entity. For this, the module provides a signed message using its device specific private key contained within. In addition,

- The message being signed is predefined i.e., not a user defined message that can be offered as service to the caller.
- This attestation specific key cannot be reused for any other purpose.
- The signature generation operation is performed during boot time before any User has a chance to interact with the module. So, the service is not handling or protecting any user data.

© 2026 IDEMIA / atsec information security.

This document can be reproduced and distributed only whole and intact, including this copyright notice.

Based on above facts it is clear that the referenced algorithms (SHA, AES-ECB, ECDSA and RSA) and services (signature generation, message digest) do not affect the security of the module, or the security of the information being protected by the module. Therefore, the module complies to exception '1b' in additional comment of IG 4.1.A.

4.4 Non-Approved Services

N/A for this module.

4.5 External Software/Firmware Loaded

The module includes a firmware load process (Manage Content service) to support necessary updates. New firmware versions within the scope of this validation must be validated through the FIPS 140-3 CMVP. Any other firmware loaded into this module is out of the scope of this validation and requires a separate FIPS 140-3 validation.

When new firmware is loaded into the module using the "Load FW with RSA DAP" and "Load FW with AES DAP" services, the Module verifies the SHA-256 digest computed over the all firmware, and the AES-CMAC authentication code computed with SD-SMAC on each block of the firmware and the SHA-256 digest. In addition to the previous method, the firmware load process verifies an RSA PSS signature computed with DAP-PUB or an AES-CMAC authentication code computed with DAP-AES key on the firmware SHA-256 digest.

© 2026 IDEMIA / atsec information security.

This document can be reproduced and distributed only whole and intact, including this copyright notice.

5 Software/Firmware Security

5.1 Integrity Techniques

The module performs an integrity test over the executable firmware loaded in non-volatile memory (NVM) (i.e. Javacard Packages) and over the ROM Code (i.e. Operating System). The integrity test uses a 16-bit CRC.

The module does not provide any services via the HMI, SFMI, HFMI, or HSMI interface that allow the operator to examine the executable code.

5.2 Initiate on Demand

The pre-operational integrity test can be performed on demand by power cycling or resetting the module. The module may perform conditional cryptographic algorithm self-tests on demand through the "Context" service.

© 2026 IDEMIA / atsec information security.

This document can be reproduced and distributed only whole and intact, including this copyright notice.

6 Operational Environment

6.1 Operational Environment Type and Requirements

Type of Operational Environment: Limited

The module is classified as a single chip hardware module running on limited modifiable firmware, the requirements of this section are not applicable.

© 2026 IDEMIA / atsec information security.

This document can be reproduced and distributed only whole and intact, including this copyright notice.

7 Physical Security

7.1 Mechanisms and Actions Required

Mechanism	Inspection Frequency	Inspection Guidance
Hard tamper-evident coating	Determined by the operator	Observe the coating surroundings of the chip for any signs of damage

Table 14: Mechanisms and Actions Required

7.2 EFP/EFT Information

The module employs environmental failure protection (EFP) for both temperature and voltage. When the EFP circuitry detects an operating temperature or voltage outside the normal operating range, the module shuts down to prevent further operation. The low and high temperature thresholds listed in Table 15 are nominal design values. The EFP temperature sensing circuit has a specified accuracy of ±3°C. As a result, the actual shutdown temperature may differ from each nominal threshold by up to 3°C in either direction.

Temp/Voltage Type	Temperature or Voltage	EFP or EFT	Result
LowTemperature	Below -25C (+/- 3C sensor accuracy)	EFP	Module stops all operations and shuts down
HighTemperature	Above 115C (+/- 3C sensor accuracy)	EFP	Module stops all operations and shuts down
LowVoltage	1.5V	EFP	Module stops all operations and shuts down
HighVoltage	6.6V	EFP	Module stops all operations and shuts down

Table 15: EFP/EFT Information

7.3 Hardness Testing Temperature Ranges

Temperature Type	Temperature
LowTemperature	-25°C
HighTemperature	115°C

Table 16: Hardness Testing Temperatures

© 2026 IDEMIA / atsec information security.

This document can be reproduced and distributed only whole and intact, including this copyright notice.

8 Non-Invasive Security

This module implements non-invasive security techniques that are not listed in SP800-140F. These techniques are mentioned in Section 12.

© 2026 IDEMIA / atsec information security.

This document can be reproduced and distributed only whole and intact, including this copyright notice.

9 Sensitive Security Parameters Management

9.1 Storage Areas

Storage Area Name	Description	Persistence Type
RAM	Volatile Memory	Dynamic
NVM	Non-volatile Memory (FLASH)	Static

Table 17: Storage Areas

9.2 SSP Input-Output Methods

Name	From	To	Format Type	Distribution Type	Entry Type	SFI or Algorithm
PIV Secure Messaging (SM) [Import]	Outside entity	NVM	Encrypted	Manual	Electronic	KTS (AES + CMAC) key wrapping/unwrapping
PIV Secure Messaging (SM) [Export]	NVM	Outside entity	Encrypted	Manual	Electronic	KTS (AES + CMAC) key wrapping/unwrapping
Global Platform Secure Channel (SC) [Import]	Outside entity	NVM	Encrypted	Manual	Electronic	KTS (AES + CMAC) key wrapping/unwrapping
Global Platform Secure Channel (SC) [Export]	NVM	Outside entity	Encrypted	Manual	Electronic	KTS (AES + CMAC) key wrapping/unwrapping
Plaintext [Import]	Outside Enttity	RAM	Plaintext	Manual	Electronic	
Plaintext [Export] (PSPs Only)	RAM	Outside entity	Plaintext	Manual	Electronic	
FIDO Key Transport [Import]	Outside Enttity	RAM	Encrypted	Manual	Electronic	KTS (AES + HMAC) key wrapping/unwrapping
FIDO Key Transport [Export]	RAM	Outside entity	Encrypted	Manual	Electronic	KTS (AES + HMAC) key wrapping/unwrapping

Table 18: SSP Input-Output Methods

© 2026 IDEMIA / atsec information security.

This document can be reproduced and distributed only whole and intact, including this copyright notice.

9.3 SSP Zeroization Methods

Zeroization Method	Description	Rationale	Operator Initiation
Global Platform TERMINATED STATE	Securely zeroizes all stored SSPs within the module. Zeroisation operation takes less than 1 second to erase all plaintext SSPs	All stored keys zeroized	By setting the module in the GLOBAL PLATFORM TERMINATED STATE
Global Platform DELETE KEY	Securely zeroizes global platform keys	Key values are zeroized, this is also followed by garbage collection to clear any values in memory	Global Platform DELETE KEY Command.
Global Platform DELETE APPLICATION	Remove an application and all its data and keys from the module	Key values are zeroized, this is also followed by garbage collection to clear any values in memory	Global Platform DELETE APPLICATION Command.
PIV PUT KEY	Zeroizes all buffers held by the key object	Values in memory overwritten	PIV PUT KEY Command.
M_CLEAR_APDU	Zeroizes the APDU buffer memory which is used as temporary memory buffer	Values in memory overwritten	Automatically upon completing the processing of a service
SELECT Context	Clears global platform session keys from memory	Values in memory overwritten	SELECT Context Command.
New key generation	Overwrites the previous key with a newly generated value.	Values in memory overwritten	Automatically upon generation of a new key
Error handling	Secure messaging keys are zeroized once an error occurs	Values in memory overwritten	Automatically upon error detection
Module Reset	Power cycles the module	The module resets overwriting the contents of SSPs stored in RAM memory	By invoking Module Reset service, or by removing power from the module
CTAP Reset	Zeroizes all CTAP SSPs back to factory default values	Values in memory overwritten	By performing the CTAP Reset service

Table 19: SSP Zeroization Methods

© 2026 IDEMIA / atsec information security.

This document can be reproduced and distributed only whole and intact, including this copyright notice.

9.4 SSPs

The table below summarizes the Sensitive Security Parameters (SSPs) that are used by the cryptographic services implemented in the module.

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
OS-DRBG-SEED	Entropy input and nonce provided by the entropy source, used to seed the Approved DRBG	256 - 256	DRBG - CSP			CTR DRBG
OS-DRBG-STATE	The current AES-128 CTR_DRBG Internal State (V, Key)	128 - 128	DRBG - CSP	CTR DRBG		CTR DRBG
SD-DAK	Security Domain Data Authentication Key (DAK) used to generate SC-ENC	256 - 256	Symmetric - CSP			AES-CMAC KBKDF SP 800-108
SD-DMK	Security Domain Data MAC Key (DMK) used to generate SC-C-MAC/SC-R-MAC	256 - 256	Symmetric - CSP			AES-CMAC KBKDF SP 800-108
SD-DEK	Security Domain Data Encryption Key (DEK) used to decrypt CSPs	256 - 256	Symmetric - CSP			AES-CBC
SC-ENC	Session key used to encrypt / decrypt Secure Channel (SC) data once Mutual Authentication is successful	256 - 256	Symmetric - CSP	KBKDF SP 800-108		AES-CBC
SC-C-MAC	Session key used to verify inbound (Command) Secure Channel (SC) data integrity	256 - 256	Symmetric - CSP	KBKDF SP 800-108		AES-CMAC

© 2026 IDEMIA / atsec information security.

This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
SC-R-MAC	Session key used to verify outbound (Response) Secure Channel (SC) data integrity	256 - 256	Symmetric - CSP	KBKDF SP 800-108		AES-CMAC
DAP-AES	Data Authentication Pattern AES Key. New firmware signature verification key	256 - 256	Symmetric - CSP			AES-CMAC
PIV-SM	PIV Secure Messaging Key Establishment Key as described in SP800-73-4 and ANSI 504-1	P-256, P-384, P-521 - 128, 192, 256	Asymmetric - CSP	ECDSA keyGen		KAS-ECC
SM-ENC	PIV Secure Messaging Key Establishment Key as described in SP800-73-4 and ANSI 504-1	128, 256 - 128, 256	Symmetric - CSP		KAS-ECC	AES-CBC
SM-C-MAC	Session key used to encrypt / decrypt Secure Messaging (SM) Data	128, 256 - 128, 256	Symmetric - CSP		KAS-ECC	AES-CMAC
SM-R-MAC	Session key used to verify data integrity of inbound (Command) Secure Messaging (SM)	128, 256 - 128, 256	Symmetric - CSP		KAS-ECC	AES-CMAC
SM-CFRM	Secure Messaging (SM) session key confirmation key	128, 256 - 128, 256	Symmetric - CSP		KAS-ECC	AES-CMAC
PIN	Card Holder Verification datum:	Variable length up	Symmetric - CSP			

© 2026 IDEMIA / atsec information security.

This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
	Authentication datum (PIN or Password) used to verify the Card Holder (User)	to 8 or 16 bytes - Variable length up to 8 or 16 bytes				
OCC-Fingerprints	Fingerprints Biometric Data extracted from the user to verify its identity	N/A - N/A	Biometric - CSP			
OCC-Facial	Facial Image Biometric Data extracted from the user to verify its identity	N/A - N/A	Biometric - CSP			
OCC-Iris	Facial Image Biometric Data extracted from the user to verify its identity	N/A - N/A	Biometric - CSP			
PUK	PIN Unblocking Code used by the PIV Application Administrator to reset the PIN	64 bits or 128 bits - 64 bits or 128 bits	Symmetric - CSP			
ADMIN_PIN	Authentication datum (PIN or Password) used to verify the PIV Application Administrator	64 bits or 128 bits - 64 bits or 128 bits	Symmetric - CSP			
ADMIN_KEY	PIV Application Administrative Key used to authenticate the PIV Application Administrator	128, 192, 256 - 128, 192, 256	Symmetric - CSP			AES-ECB
PIV-AUTH (including	PIV Authentication Key (9A) used to Authenticate the	RSA: 2048, 3072,	Asymmetric - CSP	ECDSA keyGen		ECDSA sigGen component

© 2026 IDEMIA / atsec information security.

This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
intermediate values)	PIV application in the module.Intended to be used with either RSASP1 or ECDSA primitive	4096; ECDSA P-224, P-256, P-384, P-521 - RSA: 112, 128, 150; ECDSA: 112, 128, 192, 256		RSA keyGen		RSA sigPrim
PIV-DS (including intermediate values)	PIV Digital Signature Key (9C).as described in SP800-78-4. Intended to be used with either RSASP1or ECC DSA Primitive	RSA: 2048, 3072, 4096; ECDSA P-224, P-256, P-384, P-521 - RSA: 112, 128, 150; ECDSA: 112, 128, 192, 256	Asymmetric - CSP	ECDSA keyGen RSA keyGen		ECDSA sigGen component RSA sigPrim
PIV-KMK (including intermediate values)	PIV Key Management Keys (9D) and Retired Key Management Keys ('82'to '95').as described in SP800-78-4. Intended to be used with either RSADP or ECC DH	RSA: 2048, 3072, 4096; ECDSA P-224, P-256, P-384, P-521 - RSA: 112, 128, 150; ECDSA: 112, 128, 192, 256	Asymmetric - CSP			KAS-ECC CDH Component RSA Decryption Primitive (CVL)
MUTUAL-AUTH	Mutual Authentication Key. Key type is identical to SP800-78-4 Symmetric Card	128, 192, 256 - 128, 192, 256	Symmetric - CSP			AES-ECB

© 2026 IDEMIA / atsec information security.

This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
	Authentication Key (9E), except that the key is used to enforce mutual authentication access control rules					
DS-HASH (including intermediate values)	Digital Signature key with built-in Hash (SHA2-224, SHA2-256, SHA2-384 & SHA2-512), and RSA PSS or ECDSA	RSA: 2048, 3072, 4096; ECDSA P-224, P-256, P-384, P-521 - RSA: 112, 128, 150; ECDSA: 112, 128, 192, 256	Asymmetric - CSP	ECDSA keyGen RSA keyGen		ECDSA sigVer RSA sigVer
SAM-CMAC	Symmetric key for generic CMAC computation	128, 192, 256 - 128, 192, 256	Symmetric - CSP			AES-CMAC
SAM-KDF	Symmetric Master Key used to execute the AES CMAC KDF Counter Mode derivation algorithm (as per NIST SP800-108) and retrieve the diversified key value of a target card (SAM functionality)	128, 192, 256 - 128, 192, 256	Symmetric - CSP			KBKDF SP 800-108
SAM-KDF-ENC	Symmetric Master Key used for Administrator to unlock a child PIV card	128, 192, 256 - 128, 192, 256	Symmetric - CSP			AES-CMAC

© 2026 IDEMIA / atsec information security.

This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
HOTP	HMAC-Based One-time Password (HOTP) algorithm specified in RFC 4226	160 - 160	Symmetric - CSP			HMAC
TOTP-SHA1	Time-based One-time Password (TOTP) algorithm specified in RFC 6238	160 - 160	Symmetric - CSP			SHA
TOTP-SHA256	Time-based One-time Password (TOTP) algorithm specified in RFC 6238	256 - 256	Symmetric - CSP			SHA
TOTP-SHA512	Time-based One-time Password (TOTP) algorithm specified in RFC 6238	512 - 512	Symmetric - CSP			SHA
DAP-PUB (including intermediate values)	RSA 2048 new firmware signature verification key.	2048 - 112	Symmetric - PSP			RSA sigVer
PIV-SM-PUB	The public key component used by the PIV Secure Message protocol. A superset of key types specified by SP800-78-4 is supported: P-256, P-384 and P-521 curves.	P-256, P-384, P-521 - 128, 192, 256	Asymmetric - PSP			KAS-ECC
PIV-AUTH-PUB (including intermediate values)	Public Component of PIV Authentication Key	RSA: 2048, 3072, 4096; ECDSA P-224, P-256, P-	Asymmetric - PSP	ECDSA keyGen RSA keyGen		ECDSA sigVer RSA sigVer

© 2026 IDEMIA / atsec information security.

This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
		384, P-521 - RSA: 112, 128, 150; ECDSA: 112, 128, 192, 256				
PIV-DS-PUB (including intermediate values)	Public Component of PIV Digital Signature Key	RSA: 2048, 3072, 4096; ECDSA P-224, P-256, P-384, P-521 - RSA: 112, 128, 150; ECDSA: 112, 128, 192, 256	Asymmetric - PSP	ECDSA keyGen RSA keyGen		ECDSA sigVer RSA sigVer
PIV-KMK-PUB (including intermediate values)	Public Component of PIV Key Management Keys	RSA: 2048, 3072, 4096; ECDSA P-224, P-256, P-384, P-521 - RSA: 112, 128, 150; ECDSA: 112, 128, 192, 256	Asymmetric - PSP			KAS-ECC CDH Component RSA Decryption Primitive (CVL)
DS-HASH-PUB (including intermediate values)	Public Component of Digital Signature key with built-in HashPublic Component of Digital Signature key with built-in Hash	RSA: 2048, 3072, 4096; ECDSA P-224, P-256, P-384, P-521 - RSA: 112, 128,	Asymmetric - PSP	ECDSA keyGen RSA keyGen		ECDSA sigVer RSA sigVer

© 2026 IDEMIA / atsec information security.

This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
		150; ECDSA: 112, 128, 192, 256				
FIDO-UV-PIN	PIN used within PIN/UV Auth Protocol Two for authentication	8 digits to 63 digits - 1/10^8 probability at minimum size	Symmetric - CSP			
CTAP2 ECDH-PRIV	Key agreement key within the PIN/UV auth protocol, P-256 ECDH private key	P256 - 128 bits	Asymmetric - CSP			KAS-ECC (FIDO)
CTAP2 ECDH-PUB	Public key returned by the getPublicKey() call within the PIN/UV auth protocol, P-256 ECDH public key	P256 - 128 bits	Asymmetric - PSP			KAS-ECC (FIDO)
CTAP2 SharedSecret	Shared secret computed within the PIN/UV auth protocol	P256 - 128 bits	Shared secret - CSP		KAS-ECC (FIDO)	KAS-ECC (FIDO)
CTAP2 HMAC key	Established via the PIN/UV auth protocol	128 bits - 128 bits	Symmetric - CSP		KAS-ECC (FIDO)	
CTAP2 AES key	Established via the PIN/UV auth protocol	128 bits - 128 bits	Symmetric - CSP		KAS-ECC (FIDO)	
pinUvAuthToken	HMAC key used within PIN/UV Auth Protocol Two for authentication	512 bits - 256 bits	Symmetric - CSP	CTR DRBG		HMAC
Attestation Private Key	ECDSA P-256 key used to sign	P-256 - 128 bits	Asymmetric - CSP	ECDSA keyGen		ECDSA keyGen

© 2026 IDEMIA / atsec information security.

This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
	registration requests					
Enterprise Attestation Private Key	ECDSA P-256 key used to sign registration requests	P-256 - 128 bits	Asymmetric - CSP	ECDSA keyGen		ECDSA sigGen
Discoverable Credential Private Key	ECDSA keys used for registration and verification purposes	P-256, P-384, P-521 - 128, 192, 256 bits	Asymmetric - CSP	ECDSA keyGen		ECDSA sigGen
Non-Discoverable Credential Private Key	ECDSA private key used for registration and verification purposes stored by the Relying Party instead of the applet	P-256, P-384, P-521 - 128, 192, 256 bits	Asymmetric - CSP	ECDSA keyGen		ECDSA sigGen
Attestation Public Key	ECDSA P-256 key output from the module	P-256 - 128 bits	Asymmetric - PSP	ECDSA keyGen		ECDSA sigVer
Enterprise Attestation Public Key	ECDSA P-256 key output from the module	P-256 - 128 bits	Asymmetric - PSP	ECDSA keyGen		ECDSA sigVer
Discoverable Credential Public Key	ECDSA public key used for registration and verification purposes	P-256, P-384, P-521 - 128, 192, 256 bits	Asymmetric - PSP	ECDSA keyGen		ECDSA sigVer
Non-Discoverable Credential Public Key	ECDSA public key used for registration and verification purposes stored by the Relying Party instead of the applet	P-256, P-384, P-521 - 128, 192, 256 bits	Asymmetric - PSP	ECDSA keyGen		ECDSA sigVer
Wrapping ENC Key	AES-CBC key used in wrapping	128 bits - 128 bits	Symmetric - CSP			AES-CBC

© 2026 IDEMIA / atsec information security.

This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
	and unwrapping of the key handle					
Wrapping MAC Key	HMAC key used in wrapping and unwrapping of the key handle	128 bits - 128 bits	Symmetric - CSP			HMAC

Table 20: SSP Table 1

The following table continues to summarize the Sensitive Security Parameters (SSPs) that are used by the cryptographic services implemented in the module.

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
OS-DRBG-SEED		RAM:Plaintext	Until zeroized	Module Reset	OS-DRBG-STATE:Derives
OS-DRBG-STATE		RAM:Plaintext	Until zeroized	Module Reset	OS-DRBG-SEED:Derived From
SD-DAK	PIV Secure Messaging (SM) [Import] Global Platform Secure Channel (SC) [Import]	NVM:Obfuscated	Until zeroized	Global Platform TERMINATED STATE	SC-ENC:Derives
SD-DMK	PIV Secure Messaging (SM) [Import] Global Platform Secure Channel (SC) [Import]	NVM:Obfuscated	Until zeroized	Global Platform TERMINATED STATE	SC-C-MAC:Derives SC-R-MAC:Derives

© 2026 IDEMIA / atsec information security.

This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
SD-DEK	PIV Secure Messaging (SM) [Import] Global Platform Secure Channel (SC) [Import]	NVM:Obfuscated	Until zeroized	SELECT Context Module Reset	
SC-ENC		RAM:Plaintext	Until Secure Channel closed	SELECT Context Module Reset	SD-DAK:Derived From
SC-C-MAC		RAM:Plaintext	Until Secure Channel closed	SELECT Context Module Reset	SD-DMK:Derived From
SC-R-MAC		RAM:Plaintext	Until Secure Channel closed	SELECT Context Module Reset	SD-DMK:Derived From
DAP-AES	PIV Secure Messaging (SM) [Import] Global Platform Secure Channel (SC) [Import]	NVM:Obfuscated	Until zeroized	Global Platform TERMINATED STATE Global Platform DELETE KEY	
PIV-SM	PIV Secure Messaging (SM) [Import] Global Platform Secure Channel (SC) [Import]	NVM:Obfuscated	Until zeroized	Global Platform TERMINATED STATE Global Platform DELETE KEY	SM-ENC:Derives SM-C-MAC:Derives SC-R-MAC:Derives PIV-SM-PUB:Paired With SM-CFRM:Used With

© 2026 IDEMIA / atsec information security.

This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
SM-ENC		RAM:Plaintext	Until Secure Messaging closed	New key generation Error handling Module Reset	PIV-SM:Derived From
SM-C-MAC		RAM:Plaintext	Until Secure Messaging closed	New key generation Error handling Module Reset	PIV-SM:Derived From
SM-R-MAC		RAM:Plaintext	Until Secure Messaging closed	New key generation Error handling Module Reset	PIV-SM:Derived From
SM-CFRM		RAM:Plaintext	Automatically zeroized by the module once the SM is established.	M_CLEAR_APDU Error handling Module Reset	PIV-SM:Used With
PIN	PIV Secure Messaging (SM) [Import] Global Platform Secure Channel (SC) [Import]	NVM:Obfuscated	Until changed or zeroized	Global Platform TERMINATED STATE Global Platform DELETE APPLICATION	
OCC-Fingerprints	PIV Secure Messaging (SM) [Import] Global Platform Secure Channel (SC) [Import]	NVM:Obfuscated	Until changed or zeroized	Global Platform TERMINATED STATE Global Platform DELETE APPLICATION	

© 2026 IDEMIA / atsec information security.

This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
	Plaintext [Import]				
OCC-Facial	PIV Secure Messaging (SM) [Import] Global Platform Secure Channel (SC) [Import] Plaintext [Import]	NVM:Obfuscated	Until changed or zeroized	Global Platform TERMINATED STATE Global Platform DELETE APPLICATION	
OCC-Iris	PIV Secure Messaging (SM) [Import] Global Platform Secure Channel (SC) [Import] Plaintext [Import]	NVM:Obfuscated	Until changed or zeroized	Global Platform TERMINATED STATE Global Platform DELETE APPLICATION	
PUK	PIV Secure Messaging (SM) [Import] Global Platform Secure Channel (SC) [Import]	NVM:Obfuscated	Until changed or zeroized	Global Platform TERMINATED STATE Global Platform DELETE APPLICATION	
ADMIN_PIN	PIV Secure Messaging (SM) [Import]	NVM:Obfuscated	Until changed or zeroized	Global Platform TERMINATED STATE Global Platform	

© 2026 IDEMIA / atsec information security.

This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
	Global Platform Secure Channel (SC) [Import] Plaintext [Import]			DELETE APPLICATION	
ADMIN_KEY	PIV Secure Messaging (SM) [Import] Global Platform Secure Channel (SC) [Import] Plaintext [Import]	NVM:Obfuscated	Until changed or zeroized	Global Platform TERMINATED STATE Global Platform DELETE APPLICATION PIV PUT KEY	
PIV-AUTH (including intermediate values)	PIV Secure Messaging (SM) [Import] Global Platform Secure Channel (SC) [Import] Plaintext [Import]	NVM:Obfuscated	Until changed or zeroized	Global Platform TERMINATED STATE Global Platform DELETE APPLICATION PIV PUT KEY New key generation	PIV-AUTH-PUB (including intermediate values):Paired With
PIV-DS (including intermediate values)	PIV Secure Messaging (SM) [Import] Global Platform Secure Channel (SC) [Import]	NVM:Obfuscated	Until changed or zeroized	Global Platform TERMINATED STATE Global Platform DELETE APPLICATION PIV PUT KEY New key generation	PIV-DS-PUB (including intermediate values):Paired With

© 2026 IDEMIA / atsec information security.

This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
	Plaintext [Import]				
PIV-KMK (including intermediate values)	PIV Secure Messaging (SM) [Import] Global Platform Secure Channel (SC) [Import] Plaintext [Import]	NVM:Obfuscated	Until changed or zeroized	Global Platform TERMINATED STATE Global Platform DELETE APPLICATION PIV PUT KEY New key generation	PIV-KMK-PUB (including intermediate values):Paired With
MUTUAL-AUTH	PIV Secure Messaging (SM) [Import] Global Platform Secure Channel (SC) [Import] Plaintext [Import]	NVM:Obfuscated	Until changed or zeroized	Global Platform TERMINATED STATE Global Platform DELETE APPLICATION PIV PUT KEY	
DS-HASH (including intermediate values)	PIV Secure Messaging (SM) [Import] Global Platform Secure Channel (SC) [Import] Plaintext [Import]	NVM:Obfuscated	Until changed or zeroized	Global Platform TERMINATED STATE Global Platform DELETE APPLICATION PIV PUT KEY	DS-HASH-PUB (including intermediate values):Paired With

© 2026 IDEMIA / atsec information security.

This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
SAM-CMAC	PIV Secure Messaging (SM) [Import] Global Platform Secure Channel (SC) [Import]	NVM:Obfuscated	Until changed or zeroized	Global Platform TERMINATED STATE Global Platform DELETE APPLICATION PIV PUT KEY	
SAM-KDF	PIV Secure Messaging (SM) [Import] Global Platform Secure Channel (SC) [Import]	NVM:Obfuscated	Until changed or zeroized	Global Platform TERMINATED STATE Global Platform DELETE APPLICATION PIV PUT KEY	
SAM-KDF-ENC	PIV Secure Messaging (SM) [Import] Global Platform Secure Channel (SC) [Import]	NVM:Obfuscated	Until changed or zeroized	Global Platform TERMINATED STATE Global Platform DELETE APPLICATION PIV PUT KEY	
HOTP	PIV Secure Messaging (SM) [Import] Global Platform Secure Channel (SC) [Import]	NVM:Obfuscated	Until changed or zeroized	Global Platform TERMINATED STATE Global Platform DELETE APPLICATION PIV PUT KEY	

© 2026 IDEMIA / atsec information security.

This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
TOTP-SHA1	PIV Secure Messaging (SM) [Import] Global Platform Secure Channel (SC) [Import]	NVM:Obfuscated	Until changed or zeroized	Global Platform TERMINATED STATE Global Platform DELETE APPLICATION PIV PUT KEY	
TOTP-SHA256	PIV Secure Messaging (SM) [Import] Global Platform Secure Channel (SC) [Import]	NVM:Obfuscated	Until changed or zeroized	Global Platform TERMINATED STATE Global Platform DELETE APPLICATION PIV PUT KEY	
TOTP-SHA512	PIV Secure Messaging (SM) [Import] Global Platform Secure Channel (SC) [Import]	NVM:Obfuscated	Until changed or zeroized	Global Platform TERMINATED STATE Global Platform DELETE APPLICATION PIV PUT KEY	
DAP-PUB (including intermediate values)	PIV Secure Messaging (SM) [Import] PIV Secure Messaging (SM) [Export] Global	NVM:Obfuscated	Until changed or zeroized	Global Platform TERMINATED STATE Global Platform DELETE APPLICATION PIV PUT KEY	

© 2026 IDEMIA / atsec information security.

This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
	Platform Secure Channel (SC) [Import] Global Platform Secure Channel (SC) [Export] Plaintext [Export] (PSPs Only)				
PIV-SM-PUB	PIV Secure Messaging (SM) [Import] PIV Secure Messaging (SM) [Export] Global Platform Secure Channel (SC) [Import] Global Platform Secure Channel (SC) [Export] Plaintext [Export] (PSPs Only)	NVM:Obfuscated	Until changed or zeroized	Global Platform TERMINATED STATE Global Platform DELETE APPLICATION PIV PUT KEY	PIV-SM:Paired With
PIV-AUTH-PUB (including intermediate values)	PIV Secure Messaging (SM) [Import]	NVM:Obfuscated	Until changed or zeroized	Global Platform TERMINATED STATE Global Platform DELETE	PIV-AUTH (including intermediate values):Paired With

© 2026 IDEMIA / atsec information security.

This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
	PIV Secure Messaging (SM) [Export] Global Platform Secure Channel (SC) [Import] Global Platform Secure Channel (SC) [Export] Plaintext [Export] (PSPs Only)			APPLICATION PIV PUT KEY	
PIV-DS-PUB (including intermediate values)	PIV Secure Messaging (SM) [Import] PIV Secure Messaging (SM) [Export] Global Platform Secure Channel (SC) [Import] Global Platform Secure Channel (SC) [Export] Plaintext [Export]	NVM:Obfuscated	Until changed or zeroized	Global Platform TERMINATED STATE Global Platform DELETE APPLICATION PIV PUT KEY	PIV-DS (including intermediate values):Paired With

© 2026 IDEMIA / atsec information security.

This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
	(PSPs Only)				
PIV-KMK-PUB (including intermediate values)	PIV Secure Messaging (SM) [Import] PIV Secure Messaging (SM) [Export] Global Platform Secure Channel (SC) [Import] Global Platform Secure Channel (SC) [Export] Plaintext [Export] (PSPs Only)	NVM:Obfuscated	Until changed or zeroized	Global Platform TERMINATED STATE Global Platform DELETE APPLICATION PIV PUT KEY	PIV-KMK (including intermediate values):Paired With
DS-HASH-PUB (including intermediate values)	PIV Secure Messaging (SM) [Import] PIV Secure Messaging (SM) [Export] Global Platform Secure Channel (SC) [Import] Global Platform	NVM:Obfuscated	Until changed or zeroized	Global Platform TERMINATED STATE Global Platform DELETE APPLICATION PIV PUT KEY	DS-HASH (including intermediate values):Paired With

© 2026 IDEMIA / atsec information security.

This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
	Secure Channel (SC) [Export] Plaintext [Export] (PSPs Only)				
FIDO-UV-PIN	FIDO Key Transport [Import]	RAM:Plaintext	Until changed or zeroized	Global Platform TERMINATED STATE Global Platform DELETE APPLICATION CTAP Reset	
CTAP2 ECDH-PRIV		RAM:Plaintext	Until changed or zeroized	Global Platform TERMINATED STATE Global Platform DELETE APPLICATION Module Reset CTAP Reset	CTAP2 ECDH-PUB:Paired With CTAP2 SharedSecret:Establishes
CTAP2 ECDH-PUB	FIDO Key Transport [Import]	RAM:Plaintext	Until changed or zeroized	Global Platform TERMINATED STATE Global Platform DELETE APPLICATION Module Reset CTAP Reset	CTAP2 ECDH-PRIV:Paired With CTAP2 SharedSecret:Establishes
CTAP2 SharedSecret		RAM:Plaintext	Until changed or zeroized	Global Platform TERMINATED STATE Global Platform DELETE APPLICATION Module Reset CTAP Reset	CTAP2 ECDH-PRIV:Established by CTAP2 ECDH-PUB:Established by CTAP2 HMAC key:Derives CTAP2 AES key:Derives
CTAP2 HMAC key		RAM:Plaintext	Until changed or zeroized	Global Platform TERMINATED STATE Global Platform	CTAP2 AES key:Paired With CTAP2

© 2026 IDEMIA / atsec information security.

This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
				DELETE APPLICATION Module Reset CTAP Reset	SharedSecret:Derived From
CTAP2 AES key		RAM:Plaintext	Until changed or zeroized	Global Platform TERMINATED STATE Global Platform DELETE APPLICATION Module Reset CTAP Reset	CTAP2 HMAC key:Paired With CTAP2 SharedSecret:Derived From
pinUvAuthToken		NVM:Obfuscated	Until changed or zeroized	Global Platform TERMINATED STATE Global Platform DELETE APPLICATION CTAP Reset	
Attestation Private Key		NVM:Obfuscated	Until changed or zeroized	Global Platform TERMINATED STATE Global Platform DELETE APPLICATION CTAP Reset	Attestation Public Key:Paired With
Enterprise Attestation Private Key		NVM:Obfuscated	Until changed or zeroized	Global Platform TERMINATED STATE Global Platform DELETE APPLICATION CTAP Reset	Enterprise Attestation Public Key:Paired With
Discoverable Credential Private Key		NVM:Obfuscated	Until changed or zeroized	Global Platform TERMINATED STATE Global Platform DELETE APPLICATION CTAP Reset	Discoverable Credential Public Key:Paired With

© 2026 IDEMIA / atsec information security.

This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
Non-Discoverable Credential Private Key	FIDO Key Transport [Import] FIDO Key Transport [Export]	RAM:Plaintext	Until changed or zeroized	Global Platform TERMINATED STATE Global Platform DELETE APPLICATION Module Reset CTAP Reset	Non-Discoverable Credential Public Key:Paired With
Attestation Public Key	FIDO Key Transport [Import] FIDO Key Transport [Export]	RAM:Plaintext	Until changed or zeroized	Global Platform TERMINATED STATE Global Platform DELETE APPLICATION Module Reset CTAP Reset	Attestation Private Key:Paired With
Enterprise Attestation Public Key	FIDO Key Transport [Import] FIDO Key Transport [Export]	RAM:Plaintext	Until changed or zeroized	Global Platform TERMINATED STATE Global Platform DELETE APPLICATION Module Reset CTAP Reset	Enterprise Attestation Private Key:Paired With
Discoverable Credential Public Key	FIDO Key Transport [Import] FIDO Key Transport [Export]	RAM:Plaintext	Until changed or zeroized	Global Platform TERMINATED STATE Global Platform DELETE APPLICATION Module Reset CTAP Reset	Discoverable Credential Private Key:Paired With
Non-Discoverable Credential Public Key	FIDO Key Transport [Import] FIDO Key Transport [Export]	RAM:Plaintext	Until changed or zeroized	Global Platform TERMINATED STATE Global Platform DELETE APPLICATION Module Reset CTAP Reset	Non-Discoverable Credential Private Key:Paired With

© 2026 IDEMIA / atsec information security.

This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
Wrapping ENC Key		NVM:Obfuscated	Until changed or zeroized	Global Platform TERMINATED STATE Global Platform DELETE APPLICATION CTAP Reset	Wrapping MAC Key:Paired With
Wrapping MAC Key		NVM:Obfuscated	Until changed or zeroized	Global Platform TERMINATED STATE Global Platform DELETE APPLICATION CTAP Reset	Wrapping ENC Key:Paired With

Table 21: SSP Table 2

9.5 Transitions

The use of cryptographic keys with a security strength ≥112 but <128 bits for key generation, digital signature generation, digital signature verification, KAS-ECC CDH Component, and RSA Decryption Primitive are deprecated after December 31, 2030. The use of HMAC Generation using keys ≥112 but <128 bits is acceptable through December 31, 2030, and disallowed thereafter.

© 2026 IDEMIA / atsec information security.

This document can be reproduced and distributed only whole and intact, including this copyright notice.

10 Self-Tests

The module performs the following self-tests: pre-operational firmware integrity test, conditional cryptographic algorithm test, conditional firmware load test and conditional pair-wise consistency test.

The module **does not** support any of the following self-tests: Pre-operational bypass, pre-operational critical functions test, conditional manual entry test, conditional bypass test, nor conditional critical functions test.

Determination of pass or fail of each self-test is made by the module, without external controls, externally provided input test vectors, expected output results, or operator intervention.

The module can also perform preoperational self-tests on demand for all pre-operational self-tests by power cycling the module or by calling the “Run Self-Tests” service.

10.1 Pre-Operational Self-Tests

The module performs pre-operational firmware integrity test automatically as a first action at power on. The module first performs a CAST on the cryptographic algorithm test used to perform the approved integrity technique. The module will enter the error state if the either the conditional CAST or integrity test fails or proceed to test the conditional CASTs listed in Table 25 if both passes.

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details
CRC (ROM)	16-bit CRC	EDC	SW/FW Integrity	1	Performed over all ROM code
CRC (NVM)	16-bit CRC	EDC	SW/FW Integrity	1	Performed over all executable code in NVM

Table 22: Pre-Operational Self-Tests

10.2 Conditional Self-Tests

The module performs conditional CAST prior to the algorithm’s first use. The module performs Conditional Pair-wise Consistency Tests upon generating RSA, ECDSA or ECDH asymmetric key pairs. The test is implemented by calculating a signature on predetermined data and subsequently performing a verification of the signature. If the signature cannot be verified, the generated key-pair is discarded. The module performs a conditional firmware load test when the module loads new firmware.

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
CRC	16-bit CRC	KAT	CAST	1	CAST performed prior to use of algorithm for firmware integrity test	Device power-on or reset
AES-ECB (A4945)	128-bit key	KAT	CAST	1	Decrypt	Boot Up or "Context" service

© 2026 IDEMIA / atsec information security.

This document can be reproduced and distributed only whole and intact, including this copyright notice.

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
KDF SP800-108 (A4945)	CTR mode KDF using AES-CMAC with 128-bit key	KAT	CAST	1	Key Derivation	Boot Up or "Context" service
Counter DRBG (A4945)	256-bit key	KAT	CAST	1	Instantiate, Generate, Reseed	Boot Up or "Context" service
ECDSA KeyGen (FIPS186-4) (A4945)	signature generation followed by signature verification using curve P-256	PCT	PCT	1	Sign/Verify	On ECDSA Key Generation
ECDSA SigGen (FIPS186-4) (A4945)	ECDSA Signature Generation using curve P-256	KAT	CAST	1	Sign generation comparison	First Use or "Context" service
ECDSA SigVer (FIPS186-4) (A4945)	ECDSA Signature Generation using curve P-256	KAT	CAST	1	Sign verification comparison	First Use or "Context" service
KAS-ECC Sp800-56Ar3 (A4945)	KAS-ECC using curve P-256 followed by One-step KDF	KAT	CAST	1	KAS comparison	First Use or "Context" service
HMAC-SHA2-256 (A4945)	128-bit key	KAT	CAST	1	HMAC	Boot Up or "Context" service
SHA2-256 (A4945)	N/A	KAT	CAST	1	SHA2	Boot Up or "Context" service
SHA2-512 (A4945)	N/A	KAT	CAST	1	SHA2	Boot Up or "Context" service
RSA KeyGen (FIPS186-4) (A4945)	signature generation followed by signature verification using 2048-bit key	PCT	PCT	1	Sign/Verify	On RSA Key Generation
RSA SigGen (FIPS186-4) (A4945)	Signature Generation using	KAT	CAST	1	Sign	Boot Up or "Context" service

© 2026 IDEMIA / atsec information security.

This document can be reproduced and distributed only whole and intact, including this copyright notice.

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
	PKCS1-PSS with 2048-bit key					
RSA SigVer (FIPS186-4) (A4945)	Signature Verification using PKCS1-PSS with 2048-bit key	KAT	CAST	1	Verify	First Use or "Context" service
RSA SigVer (FIPS186-4) SW/FW Load test	Signature Verification using PKCS1-PSS with 2048-bit key	CAST	SW/FW Load	1	Using RSA signature	Firmware integrity test
AES-CMAC (A4945)	AES-CMAC message authentication code using 128 bit key	Integrity Test	SW/FW Load	1	Using CMAC	Firmware integrity test
SHA2-256 SW/FW Load test	SHA2-256 performed over loaded firmware	Integrity Test	SW/FW Load	1	Message Digest	Firmware integrity test
KAS-ECC Sp800-56Ar3 (A8128)	KAS-ECC using curve P-256 followed by Two-step KDF	KAT	CAST	1	Full key agreement	First Use or "Context" service

Table 23: Conditional Self-Tests

10.3 Periodic Self-Test Information

The module has the capability to perform the pre-operational and conditional self-tests periodically. This may occur after a predefined number of -minutes passes, or, depending on the factory configuration, after invoking a predefined number of commands (APDUs).

The default configuration triggers a Periodic Self-Tests every 2 weeks of uninterrupted power. That time can be adjusted by the Application Administrator from 1 to 32767 minutes.

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
CRC (ROM)	EDC	SW/FW Integrity	Every 1 to 32767 min / After invoking 1 to 32767 APDUs	Time / Counter
CRC (NVM)	EDC	SW/FW Integrity	Every 1 to 32767 min / After invoking 1 to 32767 APDUs	Time / Counter

Table 24: Pre-Operational Periodic Information

© 2026 IDEMIA / atsec information security.

This document can be reproduced and distributed only whole and intact, including this copyright notice.

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
CRC	KAT	CAST	Every 1 to 32767 min / After invoking 1 to 32767 APDUs	Time / Counter
AES-ECB (A4945)	KAT	CAST	Every 1 to 32767 min / After invoking 1 to 32767 APDUs	Time / Counter
KDF SP800-108 (A4945)	KAT	CAST	Every 1 to 32767 min / After invoking 1 to 32767 APDUs	Time / Counter
Counter DRBG (A4945)	KAT	CAST	Every 1 to 32767 min / After invoking 1 to 32767 APDUs	Time / Counter
ECDSA KeyGen (FIPS186-4) (A4945)	PCT	PCT	Every 1 to 32767 min / After invoking 1 to 32767 APDUs	Time / Counter
ECDSA SigGen (FIPS186-4) (A4945)	KAT	CAST	Every 1 to 32767 min / After invoking 1 to 32767 APDUs	Time / Counter
ECDSA SigVer (FIPS186-4) (A4945)	KAT	CAST	Every 1 to 32767 min / After invoking 1 to 32767 APDUs	Time / Counter
KAS-ECC Sp800-56Ar3 (A4945)	KAT	CAST	Every 1 to 32767 min / After invoking 1 to 32767 APDUs	Time / Counter
HMAC-SHA2-256 (A4945)	KAT	CAST	Every 1 to 32767 min / After invoking 1 to 32767 APDUs	Time / Counter
SHA2-256 (A4945)	KAT	CAST	Every 1 to 32767 min / After invoking 1 to 32767 APDUs	Time / Counter
SHA2-512 (A4945)	KAT	CAST	Every 1 to 32767 min / After invoking 1 to 32767 APDUs	Time / Counter
RSA KeyGen (FIPS186-4) (A4945)	PCT	PCT	Every 1 to 32767 min / After invoking 1 to 32767 APDUs	Time / Counter

© 2026 IDEMIA / atsec information security.

This document can be reproduced and distributed only whole and intact, including this copyright notice.

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
RSA SigGen (FIPS186-4) (A4945)	KAT	CAST	Every 1 to 32767 min / After invoking 1 to 32767 APDUs	Time / Counter
RSA SigVer (FIPS186-4) (A4945)	KAT	CAST	Every 1 to 32767 min / After invoking 1 to 32767 APDUs	Time / Counter
RSA SigVer (FIPS186-4) SW/FW Load test	CAST	SW/FW Load	Upon loading of new firmware	N/A
AES-CMAC (A4945)	Integrity Test	SW/FW Load	Upon loading of new firmware	N/A
SHA2-256 SW/FW Load test	Integrity Test	SW/FW Load	Upon loading of new firmware	N/A
KAS-ECC Sp800-56Ar3 (A8128)	KAT	CAST	Every 1 to 32767 min / After invoking 1 to 32767 APDUs	Time / Counter

Table 25: Conditional Periodic Information

10.4 Error States

The module enters an error state upon failing any self-test. When the test fails, a special memory zone called the “Kill Card Zone” records the reason for the failure. All cryptographic functions are inhibited while the module is in an error state. The table below describes the error states in detail:

Name	Description	Conditions	Recovery Method	Indicator
Kill Card State	No further communication is possible with the module until the module is reset.	Pre-operational firmware integrity test fail any conditional self-test failure other than PCT	Resetting the module	An error code is provided through the status interface
BAD APDU	Entered when an incorrectly formatted or unknown command is received.	The module outputs a status word indicating the error condition and returns to the Idle state, clearing the error. This state includes Manage Content service firmware load attempts that fail the firmware load test; i.e., an attempt to load new firmware that fails the firmware load test will result in rejection of the	Recovers automatically after reporting the error	An error code is provided through the status interface

© 2026 IDEMIA / atsec information security.

This document can be reproduced and distributed only whole and intact, including this copyright notice.

Name	Description	Conditions	Recovery Method	Indicator
		command, and the new firmware will not be accepted by the module.		

Table 26: Error States

© 2026 IDEMIA / atsec information security.

This document can be reproduced and distributed only whole and intact, including this copyright notice.

11 Life-Cycle Assurance

11.1 Installation, Initialization, and Startup Procedures

11.1.1 Initialization

The module must have been initialized, within IDEMIA factory, to run in FIPS 140-3 level 2 mode of operation (e.g., NPIVP, CIV, etc.).

11.1.2 Startup Procedures

After manufacturing, the module is locked by a PIN Activation Code. The PIN Activation Code allows the card holder to set his or her own PIN value upon getting possession of the card. The PIN Activation Code can only be used as an authentication value for the initialization of the PIV PIN. The card holder's PIV PIN is then used for card activation.

11.2 Administrator Guidance

The module does not implement an administrator guidance.

11.3 Non-Administrator Guidance

The module does not implement a non-administrator guidance.

11.4 Design and Rules

The module enforces the following security rules:

1. The module provides three distinct operator roles: Cryptographic Officer, PIV Application Administrator and User.
2. The module provides identity-based authentication.
3. The module clears previous authentications on power cycle.
4. The module’s firmware is in executable form that does not require further compilation and there is no dynamically modified code.
5. Pre-operational Integrity self-tests do not require any operator action.
6. Data outputs are inhibited during key generation, self-tests, zeroization, and error states.
7. Status information does not contain CSPs or sensitive data that if misused could lead to a compromise of the module.
8. There are no restrictions on which keys or CSPs are zeroized by the zeroization service.
9. The module does not support a maintenance interface or role.
10. The module does not support manual key entry.
11. The module does not have any proprietary external input/output devices used for entry/output of data.
12. The module does not output intermediate key values or plaintext CSPs.

No additional interface or service is implemented by the module which would provide access to CSPs.

11.5 End of Life

The module lifecycle service can be used to set the module's status to TERMINATED. All SSPs will be zeroized upon module reset.

© 2026 IDEMIA / atsec information security.

This document can be reproduced and distributed only whole and intact, including this copyright notice.

12 Mitigation of Other Attacks

12.1 Attack List

The Module implements defenses against:

- Light attacks: The chip includes sensors to detect light attacks. A hardware attack event triggers the Kill Card behavior described below.
- Invasive fault attacks: The chip includes sensors for fault attacks. A hardware attack event triggers the Kill Card behavior described below.
- Side-channel attacks (SPA/DPA, timing analysis): The chip implements hardware countermeasures, such as induced clock jitter. The operating system enables the hardware counter measures and implements independent countermeasures in code, such as constant time execution.
- Electromagnetic attacks: This includes the defenses against side-channel attacks described above, where the detection mechanism is monitoring chip emissions rather than physical power connections. In addition, the hardware includes sensors to detect electromagnetic attacks, invoking Kill Card behavior if detected.
- Differential fault analysis (DFA): The operating system provides checks of expected conditions in areas of code deemed sensitive. If the check detects an error, the Kill Card behavior is initiated.
- Card tearing attacks: The operating system implements methods to assure protective measures are completed in the next cycle if the module loses power (i.e., is removed from the reader) before completion of the protective function.

12.2 Guidance and Constraints

The Kill Card function logs the detected attack type in a table. The table has a preset limit; when the limit is reached, the module initiates card termination, including overwrite of the CSPs, and the module is no longer operable.

© 2026 IDEMIA / atsec information security.

This document can be reproduced and distributed only whole and intact, including this copyright notice.

References

ANS X9.63-2001 **Public Key Cryptography for the Financial Services Industry, Key Agreement and Key Transport Using Elliptic Curve Cryptography**
November 20, 2001
https://webstore.ansi.org/standards/ascx9/ansix9632001

ANSI X9.62 **Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA)**
September 1999
https://webstore.ansi.org/standards/ascx9/ansix9621998

ANSI 504-1 **Information Technology - Generic Identity Command Set - Part 1: Card Application Command Set - Amendment 1**
May 2016
https://webstore.ansi.org/standards/incits/incits5042013am12016

FIDO 2.1 **Client to Authenticator Protocol (CTAP)**
June 15, 2021
https://fidoalliance.org/specs/fido-v2.1-ps-20210615/fido-client-to-authenticator-protocol-v2.1-ps-20210615.pdf

CTAP 2.1 Errata
June 21, 2022
https://fidoalliance.org/wp-content/uploads/2025/05/errata-fido-client-to-authenticator-protocol-v2.1-errata-20220621.pdf

FIPS 140-3 **FIPS PUB 140-3 - Security Requirements for Cryptographic Modules**
November 2023
https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-3.pdf

FIPS 140-3 IG **Implementation Guidance for FIPS PUB 140-3 and the Cryptographic Module Validation Program**
https://csrc.nist.gov/Projects/cryptographic-module-validation-program/fips-140-3-ig-announcements

FIPS 180-4 **Secure Hash Standard (SHS)**
March 2012
https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.180-4.pdf

© 2026 IDEMIA / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.

FIPS 186-4	**Digital Signature Standard (DSS)** July 2013 https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-5.pdf
FIPS 197	**Advanced Encryption Standard** November 2001 https://csrc.nist.gov/publications/fips/fips197/fips-197.pdf
FIPS 198-1	**The Keyed Hash Message Authentication Code (HMAC)** July 2008 https://csrc.nist.gov/publications/fips/fips198-1/FIPS-198-1_final.pdf
FIPS 201-3	**Personal Identity Verification (PIV) of Federal Employees and Contractors** January 2022 https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.201-3.pdf
FIPS 202	**SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions** August 2015 https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.202.pdf
GPC_SPE_014	**GlobalPlatform Card Technology Secure Channel Protocol '03' Card Specification v2.2 – Amendment D Version 1.1.1** July 2014 https://globalplatform.org/wp-content/uploads/2014/07/GPC_2.2_D_SCP03_v1.1.1.pdf
GPC_SPE_014	**GlobalPlatform Card Technology - Card Specification v2.3.1** March 2018 https://globalplatform.org/specs-library/card-specification-v2-3-1/
ISO 7816	**Identification cards -- Integrated circuit cards** 2004
ISO 14443	**Identification cards — Contactless integrated circuit cards** 2016
ISO 24787	**Information technology — Identification cards — On-card biometric comparison** 2010

© 2026 IDEMIA / atsec information security.

This document can be reproduced and distributed only whole and intact, including this copyright notice.

JavaCard	**JAVA CARD CLASSIC PLATFORM SPECIFICATION 3.1 CE** February 2021 https://www.oracle.com/java/technologies/javacard-downloads.html
PKCS#1	**Public Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1** February 2003 https://www.ietf.org/rfc/rfc3447.txt
SP 800-38A	**Recommendation for Block Cipher Modes of Operation Methods and Techniques** December 2001 https://csrc.nist.gov/publications/nistpubs/800-38a/sp800-38a.pdf
SP 800-38B	**Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication** May 2005 https://csrc.nist.gov/publications/nistpubs/800-38B/SP_800-38B.pdf
SP 800-38F	**Recommendation for Block Cipher Modes of Operation: Methods for Key Wrapping** December 2012 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-38F.pdf
SP 800-56Ar3	**Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography** April 2018 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-56Ar3.pdf
SP800-56B Rev2	**Recommendation for Pair-Wise Key Establishment Using Integer Factorization Cryptography** March 2019 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-56Br2.pdf
SP 800-56Cr2	**Recommendation for Key-Derivation Methods in Key-Establishment Schemes** August 2020 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-56Cr2.pdf
SP 800-73-4	**Interfaces for Personal Identity Verification – Part 1: PIV Card Application Namespace, Data Model and Representation** May 2015 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-73-4.pdf

© 2026 IDEMIA / atsec information security.

This document can be reproduced and distributed only whole and intact, including this copyright notice.

SP 800-76-2 **Biometric Specifications for Personal Identity Verification**
July 2013
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-76-2.pdf

SP 800-78-4 **Cryptographic Algorithms and Key Sizes for Personal Identity Verification**
May 2015
https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-78-4.pdf

SP 800-85A-4 **PIV Card Application and Middleware Interface Test Guidelines (SP 800-73-4 Compliance)**
April 2016
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-85A-4.pdf

SP 800-90Ar1 **Recommendation for Random Number Generation Using Deterministic Random Bit Generators**
June 2015
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-90Ar1.pdf

SP 800-90B **Recommendation for the Entropy Sources Used for Random Bit Generation**
January 2018
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-90B.pdf

SP 800-108r1 **NIST Special Publication 800-108 - Recommendation for Key Derivation Using Pseudorandom Functions**
August 2022
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-108r1.pdf

SP 800-131Ar2 **Transitioning the Use of Cryptographic Algorithms and Key Lengths**
March 2019
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-131Ar2.pdf

SP 800-133r2 **Recommendation for Cryptographic Key Generation**
June 2020
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-133r2.pdf

SP 800-140Br1 **CMVP Security Policy Requirements**
October 2022
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-140Br1.2pd.pdf

© 2026 IDEMIA / atsec information security.
This document can be reproduced and distributed only whole and intact, including this copyright notice.